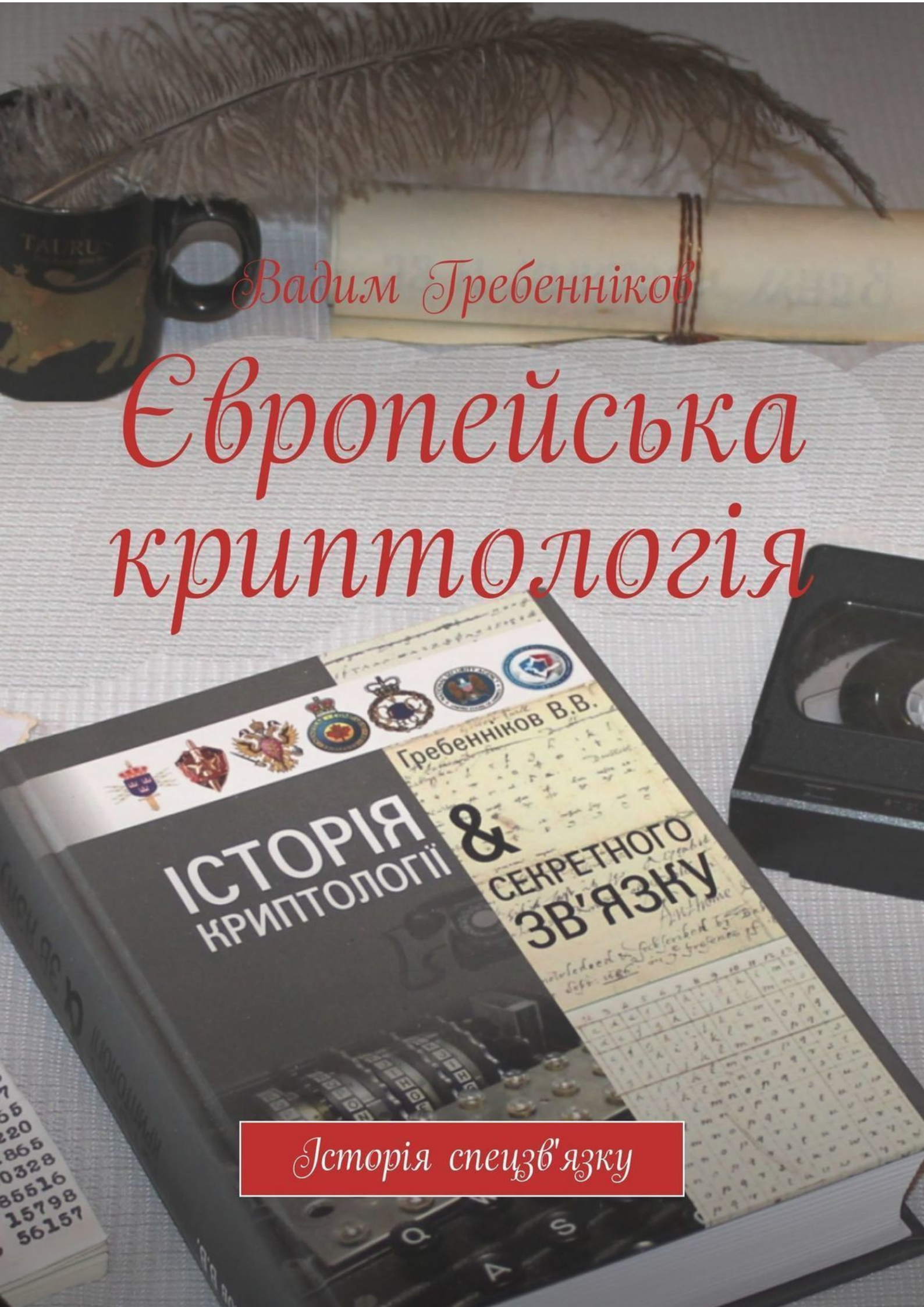
Вадим Гребенніков
Європейська криптологія
Гребенніков В.В.
ІСТОРІЯ КРИПТОЛОГІЇ & СЕКРЕТНОГО ЗВ'ЯЗКУ
Історія спецзв'язку

Вадим Гребенников

Європейська криптологія

«Издательские решения»

Гребенников В.

Європейська криптологія / В. Гребенников — «Издательские решения»,

ISBN 978-5-4493-0715-6

Книга розповідає про історію народження й розвитку криптології у країнах Європи (Великобританія, Німеччина, Швеція та інші), розробки та застосування шифрувальних і електронно-обчислювальних машин, а також утворення європейських криптологічних служб, «шпигунську» діяльність спецслужб та їхню боротьбу у «полюванні» за шифрами супротивника у контексті розвитку їхніх дипломатичних взаємовідносин. Офіційна веб-сторінка книги: http://cryptohistory.ru

ISBN 978-5-4493-0715-6

Содержание

Європейська криптологія
Історія спецзв'язку

Вадим Гребенніков

ISBN 978-5-4493-0715-6
Создано в интеллектуальной издательской системе Ridero

1. Поява шифрів

Взагалі всі шифри можуть бути розділені на два види: перестановка й заміна. При перестановці букви повідомлення просто переставляються, утворюючи анаграму. Для дуже короткого повідомлення, що складається, наприклад, з одного слова, такий спосіб досить ненадійний, оскільки існує вкрай обмежене число можливих способів перестановки жменьки букв. Так, 3 букви можуть бути розставлені всього лише 6 різними способами. Однак у міру збільшення чисельності букв кількість можливих перестановок стрімко зростає, і відновити вихідне повідомлення стає неможливо, якщо невідомий точний спосіб шифрування. Наприклад, якщо фраза складається з 35 букв, то кількість їхніх різних перестановок становить більше 50 000 000 000 000 000 000 000 000 000 000 000.

Якби одна людина змогла перевіряти одну перестановку в секунду, і якби всі люди на Землі працювали день і ніч, то, щоб перевірити всі можливі перестановки, треба було б часу в тисячі разів більше, ніж термін існування Всесвіту.

Створюється враження, що випадкова перестановка букв гарантує дуже високий ступінь безпеки, оскільки для супротивника дешифрувати навіть коротке речення виявиться нездійсненним. Однак при перестановці може утворитися неймовірно складна анаграма, і якщо букви випадково, ні з того ні із сього, переплутаються, то ні одержувач, ні перехоплювач не зможуть її розшифрувати. Тому спосіб перестановки букв повинен бути заздалегідь обговорений відправником повідомлення і його одержувачем, але разом з тим зберігатися в таємниці від супротивника.

Першим шифрувальним пристроєм, який дійшов до нас та реалізовував шифр перестановки, була так звана «скитала» або «сцитала» (близько VI—V ст. до н.е.), що використовувалась в античний період спартанцями.

Скитала являла собою дерев'яний циліндр, навколо якого намотувалася смужка шкіри або пергаменту. Відправник писав повідомлення по всій довжині скитали, а потім розмотував смужку, на якій після цього залишався безглуздий набір букв. Повідомлення виявлялося зашифрованим. Вісник брав шкіряну смужку й звичайно ховав повідомлення, використовуючи смужку як пояс, буквами усередину, тобто крім зашифровування застосовував також і стеганографію. Щоб одержати вихідне повідомлення, адресат просто намотував смужку шкіри навколо скитали того ж діаметра, що й скитала, якою користувався відправник.

У 404 році до н.е. до спартанського полководця Лісандра привели вісника, який був закривавлений та ледве тримався на ногах, одного з 5-ти вісників, що залишився живим після вкрай небезпечної подорожі з Персії. Вісник передав свій пояс Лісандру, що намотав його навколо своєї скитали й прочитав, що перський воєначальник Фарнабаз збирається напасти на нього. Завдяки скиталі Лісандр встиг підготуватися до нападу й відбив його.

Грецький історик Плутарх так описав цей спосіб шифрування: «Відправляючи до місця служби начальника флоту або сухопутного війська, ефори вручають від'їжджаючому круглий ціпок. Інший, зовсім однакової довжини й товщини, залишають собі. Ці ціпки й називають скиталами. Коли ефорам потрібно повідомити яку-небудь важливу таємницю, вони вирізують довгу й вузьку, як ремінь, смугу папірусу, щільно, без проміжків намотують її на свою скиталу й пишуть на ній текст. Потім знімають смугу й без ціпка відправляють її воєначальнику. Оскільки букви на ній розміщують без усякого зв'язку, розкидані безладно, прочитати написане він може, тільки взявши свою скиталу й намотавши на неї вирізану смугу, щоб, водячи очами навколо ціпка й переходячи від попередньої до наступної, мати перед собою зв'язне повідомлення».

Це те ж саме, начебто букви писати не підряд, а через домовлене число по кільцю доти, поки весь текст не закінчиться. Повідомлення «ВИСТУПАЙТЕ» при окружності палички в 3 букви дасть шифровку «ВУТИПЕСАТЙ».

Для прочитання шифровки потрібно було не тільки знати систему засекречування, але й мати ключ у вигляді палички визначеного діаметра. Знаючи тип шифру, але не маючи ключа, розшифрувати повідомлення було би складно. Шифр був досить популярний у Спарті й багато разів удосконалювався в пізніші часи. Про його важливе значення й велике поширення говорить свідчення Плутарха в «Порівняльних життєописах», коли історик повідомляє про життя грецького полководця Алкивіада: «Однак Лісандр звернув увагу на ці слова не раніше, ніж одержав з будинку скиталу з наказом відскіпатися від Алкивіада…»

Цей нехитрий спосіб часто використовувався через свою простоту та можливість оперативного розшифрування повідомлення. У той же час стійкість даного шифру була невелика, тому пізніше Архімед запропонував пристрій («антискитала»), за допомогою якого розшифровка подібного повідомлення без потрібного циліндра була досить простою та швидкою. Ремінь намотували на конічний «спис» і зрушували нагору й униз доти, поки не знаходили потрібний діаметр і текст повідомлення ставав зрозумілим.

Альтернативним шифру перестановки був шифр заміни, у якому кожна буква у вихідному тексті замінялася іншою буквою. Один з перших описів шифру заміни був приведений у «Камасутрі», тексті, написаному в 4-му столітті н.е. священиком-браміном Ватсьяяною, але заснованому на манускриптах, що відносяться до 4-го століття до н.е.

Згідно з «Камасутрою», жінки повинні опанувати 64 мистецтва, такі як готування їжі й напоїв, мистецтво одягання, масажу, готування ароматів. У цей список також входили менш очевидні мистецтва: чаклунство, гра в шахи, палітурна справа й теслярство. Під номером 45 у списку знаходилося мистецтво тайнопису *«mlecchita-vikalpa»,* призначене для того, щоб допомогти жінкам приховати подробиці своїх любовних зв'язків.

Один із рекомендованих способів полягав у тому, щоб розташувати попарно букви алфавіту випадковим чином, а потім заміняти кожну букву у вихідному повідомленні її парною (симетричною). Якщо застосуємо цей принцип до латинського алфавіту, то можемо скласти таку таблицю (лінійку) шифрування:

D A M H I K O Z R S U W Y

X B T. V G J. C L N E Q F. P

Тоді замість слова *«UKRAINE»* відправник напише слово *«QJNBGRS».*

На Близькому Сході один з перших шифрів заміни був розроблений древніми євреями та називався «темура» – «обмін». 22 букви єврейського алфавіту ділилися на дві частини, причому одна містилася над іншою; потім верхні букви замінялися на нижні або навпаки. Можна було встановити всілякі комбінації залежно від місця поділу алфавіту й напрямку переміщуваних букв.

Найпростіший спосіб полягав у поділі алфавіту посередині так, щоб перші дві букви, «А» і «Б», збігалися із двома останніми, «Т» і «Ш». Ці букви й дали назву методу шифрування – «Атбаш» (англ. *Atbash).* Це був простий шифр одно-алфавітної заміни для єврейського алфавіту. Таблиця (лінійка) шифрування цим методом для латинського алфавіту буде виглядати таким чином:

A B C D. E F G H I. J. K L M N O P Q R S T U V W X Y Z

Z Y X W V U T S R Q P O N M L K J. I. H G F E D. C B A

Бачимо, що у цьому шифрі заміна має симетричний вигляд. Так, наприклад, слово «UZHGOROD» перетворювалося у слово «FASTLILW».

Інший шифр «Альбам» полягав у розбивці алфавіту на дві частини та розташуванні однієї частини під іншою:

A. B C D E F G H I..J. K L M

N O P Q R S T U V W X Y Z

Слово «UZHGOROD» перетворювалося вже у слово «HMUTBEBQ».

Перше документально підтверджене використання шифру заміни у військових цілях з'явилося у «Записках про галльську війну» (лат. *Commentarii de Bello Gallico)* Гая Юлія Цезаря (I століття до н.е.). Цезар описував, як він послав повідомлення Цицерону, що перебував в облозі та був на грані капітуляції. У цьому листі латинські букви були замінені грецькими, тому ворог його не зміг би зрозуміти.

Цезар так часто користувався тайнописом, що Марко Валерій Проб написав цілий трактат про застосовувані ним шифри, який, на жаль, не дійшов до наших днів. Однак завдяки твору Гая Транквілла Светонія «Життя 12 Цезарів», написаному в 2-му столітті н.е., у нас є докладний опис одного з шифрів заміни, що застосовувалися Юлієм Цезарем. Він просто заміняв кожну букву в посланні буквою, що знаходилась в алфавіті на три позиції далі.

Ось як про це повідомляє Гай Светоній: «Існують і його листи Цицерону та листи до близьких про домашні справи: у них, якщо потрібно було повідомити що-небудь негласно, він користувався тайнописом, тобто міняв букви так, щоб з них не складалося жодного слова. Щоб розібрати й прочитати їх, потрібно читати щоразу четверту букву замість першої».

A B C D E F G H I. J. K. L M N O P Q R S T. U V W X Y Z

D E F G H I. J. K L M N O P Q R S T U V W X Y Z. A B C

Спочатку виписувався алфавіт у природному порядку, а потім під ним виписувався той же алфавіт, але зі зрушенням на 3 букви вліво. При зашифруванні буква *«A»* замінялася буквою «*D*», «*B*» замінялася на «*E*», «*C*» – на «*F*» й так далі. Так, наприклад, слово *«UZHGOROD»* перетворювалося у шифротекст *«XCKJRURG»,* а *«UKRAINE»* – у *«XNUDLQH».* Одержувач зашифрованого повідомлення шукав ці букви в нижньому рядку та по буквах над ними відновлював вихідне слово. Ключем у шифрі Цезаря була величина зрушення нижнього рядка алфавіту, тобто цифра 3. Спадкоємець Юлія Цезаря – Цезар Август – використовував той же шифр, але з ключем зрушення 4.

Вже у IV столітті до н.е. робилися спроби «механізації» криптологічної справи, пов'язані насамперед з ім'ям давньогрецького полководця Енея Тактики, захисника Трої, друга Гектора. Він створив так званий «диск Енея», що одержав у Давній Греції широке застосування. У диску діаметром 10—15 см і товщиною 1—2 см висвердлювалися отвори, що відповідали буквам алфавіту, через які просмикувалася нитка відповідно до букв шифрованого тексту. Для розшифрування нитку витягали, одержуючи зворотню послідовність букв. Цей примітивний на перший погляд спосіб шифрування був досить ефективний, тому що супротивнику, який перехопив повідомлення, було невідомо, яка буква відповідає кожному отвору. Крім того, якщо виникала небезпека перехоплення повідомлення, нитку можна було легко порвати, тим самим знищивши його.

Ідея Енея була використана при створенні й інших оригінальних шифрів заміни. Зокрема, в одному з варіантів замість диска використовувалася лінійка з кількістю отворів, рівних кількості букв алфавіту. Кожний отвір позначався своєю буквою, а букви по отворах розташовувалися в довільному порядку. До лінійки була прикріплена котушка з намотаною на неї ниткою. Поруч із котушкою був проріз. При шифруванні нитка простягалася через проріз, а потім через отвір, що відповідав першій букві шифрованого тексту, при цьому на нитці зав'язувався вузлик у місці проходження її через отвір. Потім нитка поверталася в проріз й аналогічно зашифровувалася друга буква тексту й т. д. Після закінчення шифрування нитка витягалася й передавалася одержувачу повідомлення. Той, маючи ідентичну лінійку, простягав нитку через проріз до отворів, обумовлених вузлами, і відновлював вихідний текст по буквах отворів.

Цей пристрій одержав назву «лінійка Енея». Шифр, реалізований лінійкою Енея, був одним з прикладів шифру заміни: коли букви замінялися на відстані між вузликами з урахуванням проходження через проріз. Ключем шифру був порядок розташування букв по отво-

рах у лінійці. Супротивник, що одержав нитку (навіть, маючи лінійку, але без нанесених на ній букв), не міг прочитати передане повідомлення. Аналогічне «лінійці Енея» «вузелкове письмо» отримало поширення в індіанців Центральної Америки. Свої повідомлення вони також передавали у вигляді нитки, на якій зав'язувалися різнобарвні вузлики, що визначали зміст повідомлення.

Ще один винахід стародавніх греків – так званий «квадрат Полібія». Грецький письменник Полібій (біля 200 – 120 до н.е.) використовував систему сигналізації, що була широко прийнята як метод шифрування. Він записував букви грецького алфавіту в квадратну таблицю та заміняв їх числовими координатами в таблиці номером рядка та номером стовпця. Пари чисел передавалися за допомогою смолоскипів. У варіанті з латинським алфавітом для передачі, наприклад, букви «*U*» потрібно було взяти 4 смолоскипи в праву руку та 5 – у ліву, або записати як цифру «45» (див. таблицю).

	1	**2**	**3**	**4**	**5**
1	A	B	C	D	E
2	F	G	H	I,J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Наприклад, слово *«UKRAINE»* можна записати як цифровий шифротекст «45254211243315» або «54522411423351».

Цікаво, що шифр Полібія дійшов до наших днів та одержав своєрідну назву «шифру в'язнів». Для його використання потрібно було тільки знати природний порядок розташування букв алфавіту (як у вищезазначеному прикладі для англійської мови). Число 3, наприклад, передавалося шляхом потрійного стукоту. При передачі букви спочатку відстукувалося число номера рядка, у якому знаходилася буква, а потім число номера відповідного стовпця. Наприклад, буква «*F*» передавалася подвійним стукотом (другий рядок) і потім одинарним (перший стовпець).

Із застосуванням цього шифру пов'язані деякі історичні казуси. Так, російські *«декабристы»,* які були ув'язнені після невдалого повстання, не змогли встановити зв'язок з князем Одоєвським. Виявилося, що він (добре освічений за тих часів) не пам'ятав природний порядок розташування букв у російському та французькому алфавітах (іншими мовами він не володів). «*Декабристы*» для російського алфавіту використовували прямокутник розміру 5х6 (5 рядків та 6 стовпців) і скорочений до 30 букв алфавіт.

Пізніше букви стали розташовувати в квадраті хаотично, але це вимагало наявність такого квадрата у отримувача повідомлення, що також було небезпечно. Вихід був знайдений у застосуванні так званого ключового слова, що легко запам'ятовувалося. Обиралося недовге слово (наприклад, «*UKRAINE*»), з нього забиралися букви, що повторювалтся, а ті, що залишалися, записувалися в перші клітини квадрата по рядках. Порожні клітини заповнювалися буквами алфавіту, що залишилися, у природному порядку (див. таблицю).

	1	2	3	4	5
1	U	K	R	A	I
2	N	E	B	C	D
3	F	G	H	L	M
4	O	P	Q	S	T
5	V	W	X	Y	Z

В результаті такого шифрування слово *«UZHGOROD»* перетворюється у цифровий шифротекст «11553332414125».

Полібійський квадрат став однією з найбільш широко розповсюджених криптосистем, що вживалися у той час. Цьому сприяла його досить висока стійкість (у всякому разі, до автоматизації дешифрувальних систем): квадрат 5х5 для латинського алфавіту містить 155112100433310000000000000 (розрахунок досить приблизний) можливих положень, що практично виключає його дешифрування без знання ключа.

Ледащі й тому винахідливі римляни в IV столітті до н.е., щоб спростити процедуру шифрування, почали застосовувати два шифрувальні диски. Кожний із дисків, розміщених на загальної вісі, містив на своєму ободі алфавіт у випадковій послідовності. Кожній букві першого диска відповідала буква другого, що й становило шифр. Знайшовши на одному диску букву тексту, з іншого диска зчитували відповідну їй букву шифру. Такі прилади, що породжували шифр простої заміни, використовувалися аж до епохи Відродження.

Ці криптосистеми активно застосовувалися в Давній Греції та Римі й надовго визначили характер криптології. В умовах потреби ручного розшифрування, полібійський квадрат був практично невразливим шифром, а скитала та диск Енея були досить прості, проте дозволяли оперативно зашифровувати й розшифровувати інформацію, що робило їх вигідними, скажімо, в польових умовах для оперативної передачі наказів.

Із занепадом античної цивілізації та утворенням у Європі варварських держав, криптологія занепала. Велика шкода її розвитку була завдана в часи середньовічної інквізиції. Всі кращі досягнення цивілізації, а разом з ними й криптологія, були втрачені. За свідченням святого Джерома «увесь світ поринув у руїни». В умовах, коли грамотність була вкрай низька, зашиф-

ровувати повідомлення не було необхідності, тому й самих письмових повідомлень практично не було.

Так, король франків Карл Великий, засновавший у 800 році Священну Римську імперію, навчився читати й писати тільки у 50 років. Проте Карл Великий знав і використовував у листуванні зі своїми генералами шифр заміни букв алфавіту групою символів.

Освіта й грамотність у ті часи зосередилися в церкві, тому тайнопис став її монополією. Церква ухвалила, що простим парафіянам не можна приховувати таємниці від «Господа», а тайнопис – це «єресь». За використання тайнопису передбачалися жорстокі заходи покарання, аж до страти.

Крім вищеперерахованих причин, криптологія перебувала в занепаді ще й тому, що в ній бачили елементи чаклунства. Набір незрозумілих букв або символів, сам по собі схожий на заклинання, сприймався як щось магічне, а люди, що розуміли у цьому наборі символів зміст, розцінювалися як чаклуни або ворожки, що не могло не накласти свій відбиток на ставлення до них у християнській Європі.

З перших днів свого існування криптологія мала на меті сховати зміст важливих розділів письмових документів, що мали відношення до таких сфер магії, як гадання й заклинання. В одному з рукописів про магію, що датується III століттям н.е., був використаний шифр, щоб сховати важливі частини чаклунських рецептів. Криптографія часто була на службі магії в часи середньовіччя, і навіть в епоху Відродження за допомогою шифрів алхіміки засекречували важливі частини формул одержання «філософського каменя».

До шифрування інформації «призивалися» містичні сили. Так, наприклад, рекомендувалося використовувати «магічні квадрати». У квадрат розміром 4 х 4 вписувалися числа від 1 до 16. Його магія полягала в тому, що сума чисел по рядках, стовпцях і діагоналях дорівнювала одному й тому ж числу – 34. Уперше ці квадрати з'явилися в Китаї, де їм і була приписана деяка «магічна сила» (див. таблицю).

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

Для зашифрування слова «ЗАКАРПАТТЯ» букви вписувалися послідовно до квадрату згідно з записаними в них цифрами, а до пустих клітинок вписувалися будь-які букви (див. таблицю).

16 Ж	3К	2А	13Г
5Р	10Я	11Б	8Т
9Т	6П	7А	12В
4А	15Е	14Д	13

Після цього букви записувалися у рядок і отримувався такий шифротекст: ЖКАГРЯБТТПАВАЕДЗ. Даний шифр – це звичайний шифр перестановки, але вважалося, що особливу стійкість йому надають чари «магічного квадрата».

На перший погляд здається, начебто магічних квадратів дуже мало. Проте їхнє число дуже швидко зростає зі збільшенням розміру квадрата. Так, існує лише один магічний квадрат розміром 3х3, якщо не брати до уваги його повороти. Магічних квадратів 4х4 налічується вже 880, а число магічних квадратів розміром 5х5 близько 250000. Тому магічні квадрати більших розмірів могли бути гарною основою для надійної системи шифрування того часу, тому що ручний перебір всіх варіантів ключа для цього шифру був немислимий.

Подібність між магією та криптологією обумовлювалася й іншими факторами. Крім криптології, таємничі символи використовувалися в зрозумілих лише присвяченим сферах магічних знань – астрологія та алхімія, де подібно знакам відкритого тексту, кожна планета й кожна хімічна речовина мали спеціальний знак. Як і зашифровані слова, заклинання й магічні формули, начебто «абракадабри», нагадували нісенітницю, але в дійсності мали важливе значення.

Те, що писали або малювали астрологи та маги, було схоже на кодограму, де кожний символ або ієрогліф мав своє особисте як екзотеричне (матеріальне), так і езотеричне (духовне) значення. Наприклад, символ Сонця – це індивідуальність та духовність, Місяця – м'якість та душевність, Меркурія – мислення та інтелектуальність, Венери – жіночість та кохання, Марса – мужність та активність, Юпітера – законослухняність та релігійність, Сатурна – самотність та цілеспрямованість тощо. Навіть місця символів, де вони були намальовані, теж визначали їх вплив на події життя та взаємовідносини з іншими чинниками долі. А те, що одним малюнком (гороскопом) можна відобразити долю та все життя людини або країни, здавалося справжньою магією чи чаклунством.

Думка про те, що криптоаналіз є також за своєю суттю якоюсь магією, складалася у зв'язку з поверхневою подібністю криптоаналізу та гадання. Добування істинного змісту з шифротексту здавалося точно такою ж справою, що й одержання знань шляхом вивчення розташування зірок і планет, довжини ліній і місць їхнього перетинання на долоні, нутрощів овець, положення кавового осаду в чашці. Видимість брала гору над реальністю. Простодушні люди бачили магію навіть у звичайному процесі розшифрування. Інші бачили її в криптоаналізі, тому що розкриття чогось глибоко захованого здавалося їм незбагненним і надприродним.

Не таким сильним був занепад криптології у Візантії, що зберегла багато античних традицій. Але й тут криптосистеми дуже спростилися та були легко вразливими. Найчастіше повідомлення просто писали у зворотньому порядку або заміняли кожну букву на наступну за алфавітом. Для засекречування повідомлень також використовували маловідомі іноземні мови, найчастіше вірменську або давньоєврейську. Але в цілому, у порівнянні з епохою античності, криптологія перебувала на вкрай низькому рівні.

В середньовічному Китаї у трактаті «Основи класичної військової науки», складеному в XI столітті нашої ери, були присутні лише кодувальні рекомендації. В них рекомендувалося співвіднести з різними простими повідомленнями перші 40 знаків якого-небудь вірша, відомого як відправнику, так і одержувачу. По першому знаку вірша, поставленому в домовленому місці цілком безневинного повідомлення, одержувач «зчитував» інформацію, наприклад, що потрібно послати більше провіанту. Такі коди практично не піддавалися розшифруванню, але вони могли використовуватися лише в дуже обмеженому масштабі.

Деякі окремі релігійні організації використовували особистий алфавіт як одно-алфавітний шифр заміни. Так, шифри тамплієрів і розенкрейцерів були дуже схожими та знайшли своїх шанувальників в особі масонів (деякі дослідники, зокрема, О.П.Блаватська, так їх і називали – «масонський»). Масонський шифр використовувався їхніми «ложами» для таємного листування між присвяченими вищих ступенів.

У XVIII столітті франкмасонами використовувався для забезпечення таємності своїх документів так називаний шифр «*Pigpen*». У ньому кожна буква замінялася визначеним символом таким чином: щоб зашифрувати букву, визначалося її місцезнаходження в одній з чотирьох сіток, а потім малювалася та частина сітки, що відповідала цій букві.

2. Становлення криптології як науки

В арабському світі криптологія не тільки не занепала, але продовжувала успішно розвиватися, досягши значних успіхів. Про тайнопис і його значення говорилося навіть у казках «Тисячі й однієї ночі». У 855 році арабський письменник, алхімік і єгиптолог Абу Бакр Ахмед ібн Вахш (Ахмад Бін Абубекр Бін Вахіші) описав відомі йому класичні шифралфавіти у своїй «Книзі про велике прагнення людини розгадати загадки давньої писемності» (араб. *Kitab Shawq al-Mustaham).* Видання арабського тексту з англійським перекладом з'явилося лише у 1806 році.

Це була одна з перших книг про криптографію з описами декількох шифрів, зокрема із застосуванням декількох алфавітів, де автор також обговорює деякі давні писемності та стверджує про дешифрування єгипетських ієрогліфів. Один із шифралфавітів, що називався «дауді» (на ім'я ізраїльського царя Давида), використовувався для зашифрування трактатів з «чорної» магії. Він був складений з видозмінених букв давньоєврейського алфавіту.

Крім того, найбільш ранній із відомих описів методу використання частоти появи букв з метою «злому» шифрів належав перу арабського вченого Абу Юсуф Якуб ібн Ісхак ібн Сабах аль-Кінді (біля 800—879) та датований приблизно 850 роком. Відомий як «філософ арабського світу», аль-Кінді був автором 290 книг з медицини, астрономії, математики, лінгвістики й музики. Його найзнаменитіший трактат, що був виявлений заново лише у 1987 році в оттоманському архіві Сулайманія в Стамбулі, називався «Трактат про дешифрування криптографічних повідомлень аль-Кінді». Хоча в ньому був викладений докладний аналіз статистики, фонетики й синтаксису арабської мови, революційна система криптоаналізу аль-Кінді вміщається у два короткі абзаци:

«Один із способів прочитати зашифроване повідомлення, якщо ми знаємо мову, якою воно написано, – це взяти інший незашифрований текст на тій же мові, розміром приблизно на сторінку, і потім підрахувати появу в ньому кожної з букв. Назвемо букву, що найбільш часто зустрічається, «першою», букву, що за частотою появи знаходиться на другому місці, назвемо «другою», букву, що за частотою появи знаходиться на третьому місці, назвемо «третьою» і так далі, поки не будуть пораховані всі різні букви в незашифрованому тексті.

Потім подивимося на зашифрований текст, що ми хочемо прочитати, і таким же способом проведемо сортування його символів. Знайдемо символ, що найбільш часто зустрічається, і замінимо його «першою» буквою незашифрованого тексту, другий за частотою появи символ замінимо «другою» буквою, третій за частотою появи символ замінимо «третьою» буквою й так далі, поки не будуть замінені всі символи зашифрованого повідомлення, що ми хочемо дешифрувати».

Але по-справжньому характеризує пізнання арабів у сфері криптології енциклопедія з 14-ти томів «Шауба аль-Аша» (Світоч для незрячого в ремеслі писаря), що була написана вченим Шихабом ад-Дін Абу-л-Абас Ахмад ібн Алі ал-Калкашанді (1335—1418) у 1412 році. У розділі «Щодо приховання букв таємних повідомлень», автор виклав всі відомі йому на той час існуючі в арабському світі криптосистеми. Він містив дві частини: одна стосувалася символічних дій і натяків, а інша була присвячена симпатичному чорнилу та криптології.

У роботі пропонувалося сім систем шифрування, що повторювали неопубліковані ідеї його попередника Ібн ад-Дурайхима (1312—1361), який був першим, хто використав частотний аналіз букв:

– замінювати одну букву іншою;
– писати слово у зворотному порядку;
– переставляти у зворотному порядку букви слів;
– замінювати букви на цифри згідно з прийнятою заміною арабських букв на числа;

– замінювати кожну букву відкритого тексту на дві арабські букви, які використовуються і як числа й сума яких дорівнює цифровій величині букви відкритого тексту, що шифрується;

– замінювати кожну букву на ім'я якої-небудь людини;

– використовувати словник заміни, що описує положення Місяця, назви країн (у певному порядку), назв фруктів, дерев тощо.

Першого разу за всю історію шифрів в енциклопедії приводився список як систем перестановки, так і систем заміни. Більше того, у п'ятому пункті списку вперше згадувався шифр, для якого була характерна більш ніж одна заміна букв відкритого тексту. Однак яким би чудовим та важливим цей факт не був, він затьмарюється першим в історії описом криптоаналітичного дослідження шифротекста.

Його джерела, мабуть, варто шукати в інтенсивному й скрупульозному вивченні Корану численними школами арабських граматиків. Поряд з іншими дослідженнями вони займалися підрахунком частоти появи слів, намагаючись скласти хронологію глав Корана, вивчали фонетику слів, щоб установити, чи були вони справді арабськими або були запозичені з інших мов. Більшу роль у виявленні лінгвістичних закономірностей, що призвели до виникнення криптоаналізу в арабів, зіграв також розвиток лексикографії. Адже при складанні словників авторам фактично доводилося враховувати частоту появи букв, а також те, які букви можуть стояти поруч, а які ніколи не зустрічаються по сусідству.

Калкашанді писав у своїй книзі: «Якщо ви хочете прочитати повідомлення, що ви одержали в зашифрованому вигляді, то насамперед почніть підрахунок букв, а потім порахуйте, скільки разів повторюється кожен знак, і підбийте підсумок у кожному окремому випадку. Якщо винахідник шифру був дуже уважний та сховав у повідомленні всі границі між словами, то перша задача, що повинна бути вирішена, полягає в перебуванні знака, що розділяє слова. Це робиться так: ви берете букву та працюєте, виходячи з припущення, що наступна буква є знаком, що поділяє слова. І в такий спосіб ви вивчаєте все повідомлення з урахуванням різних комбінацій букв, з яких можуть бути складені слова… Якщо виходить, тоді усе в порядку; якщо ні, то ви берете наступну букву і т.д., поки ви не зможете установити знак розділу між словами. Потім потрібно знайти, які букви найчастіше трапляються у повідомленні, та порівняти їх зі зразком частоти появи букв, про яке згадувалося колись. Коли ви побачите, що одна буква трапляється частіше, ніж інші у даному повідомленні, ви припускаєте, що це буква „аліф“. Потім ви припускаєте, що наступна за частотою появи буде буквою „лам“. Точність вашого припущення повинна підтверджуватися тим фактом, що в більшості контекстів буква „лам“ випливає за буквою „аліф“… Потім перші слова, що ви спробуєте розгадати у повідомленні, повинні складатися з двох букв. Це робиться шляхом оцінки найбільш ймовірних комбінацій букв доти, поки ви не переконаєтеся в тому, що ви знаходитеся на правильному шляху. Тоді ви дивитеся на їхні знаки і виписуєте їхні еквіваленти кожного разу, коли вони трапляються у повідомленні. Потрібно застосовувати точно такий же принцип стосовно трибуквених слів цього повідомлення, поки не переконаєтеся, що на щось натрапили. Ви виписуєте еквіваленти з усього повідомлення. Цей же принцип застосовується стосовно слів, що складають з чотирьох і п'яти букв, причому метод роботи такий же. Коли виникає який-небудь сумнів, потрібно висловити два-три припущення або ще більше і виписати кожне з них, поки воно не підтвердиться на підставі іншого слова».

Давши це чітке пояснення, Калкашанді наводить приклад розкриття шифру. Дешифрована криптограма складається з двох віршованих рядків, зашифрованих за допомогою умовних символів. На закінчення Калкашанді відзначив, що вісім букв не було використано і що це саме ті букви, що знаходяться наприкінці переліку, складеного за частотою появи. Він підкреслив: «Однак це проста випадковість: буква може бути поставлена не на те місце, що вона повинна займати у вищезгаданому переліку». Таке зауваження свідчить про наявність великого досвіду в сфері криптоаналізу. Щоб розставити всі крапки над «і», Калкашанді приво-

дить другий приклад криптоаналізу досить довгої криптограми. Цим прикладом він і закінчив розділ із криптології.

Араби першими звернули увагу на можливість використання стандартних слів і виразів для дешифрування. Так, перший широко відомий філолог серед арабів Ха-ліль ібн Ахмад аль-Фарахіді (біля 718—791), дешифрувавши криптограму грецькою мовою, надіслану йому візантійським імператором, заявив: «Я сказав собі, що лист повинен починатися зі слів „В ім'я Бога“ або як-небудь у цьому роді. Отже, я склав на основі цього перші букви, і все виявилося правильним». На основі відкритого ним методу дешифрування він написав книгу «Кітаб аль-маумма» (Книга таємної мови).

Історія замовчує те, як араби використали свої блискучі криптоаналітичні здібності, продемонстровані Калкашанді, для розкриття військових і дипломатичних криптограм, або який вплив це зробило на мусульманську історію. Однак зрозуміло, що незабаром ці знання перестали застосовуватися на практиці та були забуті. Один епізод, що відбувся майже 200 років по тому, яскраво демонструє ту деградацію у сфері криптоаналізу, що відбулася за той час.

У 1600 році мароканський султан Ахмед аль-Мансур направив до англійської королеви Єлизавети I посольство на чолі з довіреною людиною – міністром Абдель Вахід ібн Масуд ібн Мухамед Ануном. Посольство повинне було укласти з Англією союз, спрямований проти Іспанії. Анун відправив на батьківщину зашифровану простою заміною депешу, яка незабаром після цього якимось чином потрапила в руки одного араба. Араб той був, можливо, розумною людиною, але, на жаль, він нічого не знав про велику арабську спадщину у сфері криптоаналізу. Свідчення тому -пам'ятна записка, у якій він написав:

«Хвала Аллаху! Щодо листа міністра Абдель Вахід ібн Масуд ібн Мухамед Ануна. Я знайшов лист, написаний його рукою, у якому він за допомогою таємних знаків виклав деякі відомості, призначені для нашого заступника Ахмеда аль-мансура. Ці відомості стосуються султанші християн (хай покарає їх Аллах!), що жила в країні за назвою Лондон… З того моменту, як цей лист потрапив до мене, я постійно час від часу вивчав знаки, що містилися в ньому. Пройшло приблизно 15 років, поки не настав той час, коли Аллах дозволив мені зрозуміти ці знаки, хоча ніхто не навчав мене цьому…».

Відмітимо, що для таке завдання Калкашанді виконав би не за 15 років, а за кілька годин!

Невідомо, чи був тісний зв'язок між розвитком європейської та східної криптології. Безумовно подібного роду контакти могли відбуватися в Іспанії й під час Хрестових походів, але стверджувати, що європейська криптологія в той час використала арабський досвід, не можна. Праці Калкашанді не були перекладені з арабської мови, тому прямого зв'язку європейської криптології зі східною немає. Крім того, якщо на сході криптологія була скоріше частиною лінгвістики, то в Європі вона була ближче до математики й природничих наук, що також визначило її специфіку.

Європейська цивілізація почала користуватися криптологією з часів середньовічного феодалізму. Правда, спочатку тайнопис знаходився в зародковому стані, його застосовували рідко і мінливо. Навіть, церковні системи шифрування були простими, хоча в ту епоху церква користувалася найбільшим впливом у суспільстві. Цікаво, що в той час, коли прості люди шифрування вважали чаклунством, основні роботи в сфері криптології виконувалися в лоні католицької церкви.

У X столітті чернець Герберт Орильякський (Аврилакський), що правив католицькою церквою під ім'ям папи Сильвестра II (біля 946—1003) і вивчав «магічні» знання, вів записи за стенографічною системою, створеною Марком Туллієм Тіроном (103—4 до н.е.), вільновідпущеним і другом відомого Цицерона.

У 1267 році англійський монах-францисканець, професор в Оксфорді, універсальний вчений, математик, оптик, астроном Роджер Бекон (1214—1294) написав першу європейську книгу, яка була присвячена криптології та називалася «Послання ченця Роджера Бекона про

таємні дії мистецтва і природи та нікчемність магії» (лат. *Epistola fratris Rogerii Baconis de secretis operibus artis et naturae, et de nullitate magiae).* У передмові він помітив: «Дурень той, хто пише про таємницю яким-небудь способом, але не так, щоб приховати її від простолюду».

У розділі «Сім способів захования таємниці» Бекон привів такі методи шифрування: повна заміна символів і знаків, використання загадкових і образних виразів, особливі способи запису, одночасне використання букв різних мов, застосування різних малюнків, скорочення голосних букв тощо. За свої наукові праці він був засуджений за «чорну магію» церковним судом і провів 14 років в ув'язненні.

У 1379 році антипапа Климент VII, який за рік до цього втік до французького Авіньону, звелів своїй канцелярії ввести в дію нові шифри. Секретар антипапи Габріель де Лавінда, що працював у його представництві в одному з північно-італійських міст-держав, виготовив індивідуальні ключі для всіх 24 кореспондентів антипапи. Ключі де Лавінда, що були найдавніші серед збережених на Заході, поєднували у собі елементи коду й шифру.

У своїй книзі «Трактат про шифри» Габріель де Лавінда описав новий тип шифру, що використовував «омофони», тобто припускав заміну букв декількома символами (знаками), кількість яких пропорційна появі букв у відкритому тексті. Імена, посади, географічні назви він рекомендував заміняти спеціальними знаками. Крім шифроалфавіту заміни з «пустишками» майже кожен такий ключ включав невеликий список з десятка широко розповсюджених слів або імен, яким приводилися у відповідність двобуквені кодові еквіваленти. Це самий ранній зразок «Номенклатора» – гібридної системи шифрування, який у наступні 450 років поширився по всій Європі.

Розвитку європейської криптології сприяло те, що середньовічні вчені, зробивши відкриття, аж ніяк не поспішали описати його в листах колегам, як це було тоді прийняте за відсутності періодичних наукових видань. Нерідко ту частину відкриття, що тепер називають «*know how*», вони шифрували анаграмою, переставляючи букви повідомлення за відомим тільки їм ключем. Наприклад, назви древньої та сучасної столиць Японії в російському написанні теж являють собою анаграму: КІОТО – ТОКІО.

Пояснюючи широке поширення тайнопису серед вчених середньовіччя, О.І.Герцен писав: «Гнані, блукачі із країни в країну, оточені небезпеками, вони не зарили з розсудливого страху істини, про яку були покликані свідчити; вони висловлювали її скрізь, де не могли висловлювати прямо – одягали її в маскарадне плаття, наділяючи алегоріями. Ховали під умовними знаками, прикривали тонким флером, що для когось проникливого нічого не приховувало, але приховувало від ворога: любов догадлівіша й проникливіша ненависті. Іноді вони це робили, щоб не злякати боязкі душі сучасників; іноді – щоб не потрапити на багаття».

Найбільшого розквіту криптологія досягла в період Епохи Відродження. Творчі періоди життя таких великих людей, як Леонардо да Вінчі, кардинала Рішельє, Лю-овиків XII—XIV й інших дали поштовх до зародження наукового підходу до проблем тайнопису. Саме в ці роки виникло поняття «кодування» повідомлень, тобто заміни букв і цифр відкритого тексту на букви, цифри, знаки, згідно із заздалегідь обумовленим правилом, законом.

Леонардо да Вінчі (1452—1519) також шифрував більшість своїх особистих записів. Найпростіший вид шифру, яким він користувався, це зворотнє (дзеркальне) написання тексту так, що прочитати його можна було лише у відбитті дзеркала, наприклад: слово *«UKRAINE»* перетворюється у шифротекст *«ENIARKU».* Однак Леонардо іноді використовував й більш серйозні шифри, тому далеко не всі його замітки та записи розшифровані й вивчені до цього часу. Невипадково вийшли в світ книга та фільм з назвою «Код да Вінчі».

Одним із провідних європейських криптологів був відомий англійський письменник, астроном-аматор, митний чиновник Джеффрі Чосер (1343—1400). В 1370-х роках він виконував секретні дипломатичні доручення свого короля в Італії й Франції. Все таємне листування

Чосер здійснював, використовуючи шифр простої заміни. Його книга «Екватор Планет», що вийшла у 1390 році, містила окремі шифровані глави.

У 1401 році в Мантуанському герцогстві був знайдений шифр із використанням «омофонів» для голосних букв. Той факт, що «омофони» застосовувалися не для всіх букв, а тільки для голосних, свідчив про знання криптоаналітичних методів, заснованих на частоті появи знаків шифротекста.

Широкий розвиток торгівлі в середині століття спровокував появу специфічних шифрів, дуже простих і зручних, якими могли б користуватися купці для передачі, наприклад, дати приїзду або ціни товару. Це були прості шифри заміни цифр на букви, засновані на ключовому слові. Торговці заздалегідь домовлялися про використання загального ключового слова, букви якого відповідали б цифрам.

Наприклад, для ключа «ШИФРОВАНИЙ» цифра 0 означає букву «Ш», цифра 1 означає «И», 2 – «Ф», 3 – «Р» тощо. Тому одержавши від кореспондента повідомлення «ПРИБУВАЮ ИФШАЙР», вони його читали як «ПРИБУВАЮ 12/06/93». Простота та зручність цієї системи шифрування дозволили їй дожити до початку минулого століття без усяких змін. Крім цих шифрів, найчастіше використовувався шифр простої заміни, що полягав у заміні кожної букви повідомлення на відповідну їй букву шифру.

У ручних шифрах того часу часто використовувалися таблиці, які давали прості шифри перестановки. Ключем у них служив розмір таблиці та фраза, що задавала перестановку або спеціальну особливість таблиць. Проста перестановка без ключа – один із найпростіших методів шифрування, родинний шифру «скитала».

Наприклад, повідомлення «ЗУСТРІЧАЙ У ДЕСЯТЬ» записувалося в таблицю розміром 4х4 по стовпцях (див. таблицю).

З	Р	Й	С
У	І	У	Я
С	Ч	Д	Т
Т	А	Е	Ь

Після того, як відкритий текст був записаний по стовпцях, для утворення шифровки він зчитувався по рядках. В результаті виходив шифротекст: «ЗРЙСУ-ІУЯСЧДТТАЕЬ». Для використання цього шифру відправнику та одержувачу потрібно було домовитися про загальний ключ у вигляді розміру таблиці. Об'єднання букв у групи не входило у ключ шифру та використовувалося лише для зручності запису тексту.

Більш практичним був метод шифрування, який був названий одиночною перестановкою за ключем. Він відрізнявся від попереднього лише тим, що стовпці таблиці переставлялися за ключовим словом, фразою або набором чисел довжиною в рядок таблиці. Ключове слово (наприклад, «ШИФР») вписувалося у перший рядок таблиці, та здійснювалася перестановка стовпців відповідно до порядкових номерів букв ключа (див. таблицю).

Ш	И	Ф	Р					
4	1	3	2		1	2	3	4
З	Р	Й	С	→	Р	С	Й	З
У	І	У	Я		І	Я	У	У
С	Ч	Д	Т		Ч	Т	Д	С
Т	А	Е	Ь		А	Ь	Е	Т

В результаті зчитування по рядках повідомлення «ЗУСТРІЧАЙ У ДЕСЯТЬ» перетворялося у шифротекст «РСЙЗІЯУУЧТДСАЬЕТ».

Крім одиночних перестановок використовувалися ще подвійні перестановки стовпців і рядків таблиці з повідомленням згідно з попередньо визначеним порядком нумерування рядків і стовпців таблиці, що й було ключем шифру. При цьому перестановки визначалися окремо для стовпців та окремо для рядків. У таблицю вписувався текст по стовпцях, після чого здійснювалися перестановки стовпців та рядків (див. таблицю).

	3	2	4	1			1	2	3	4			1	2	3	4
2	З	Р	Й	С		2	С	Р	З	Й		1	Я	І	У	У
1	У	І	У	Я	→	1	Я	І	У	У	→	2	С	Р	З	Й
4	С	Ч	Д	Т		4	Т	Ч	С	Д		З	Ь	А	Т	Е
3	Т	А	Е	Ь		3	Ь	А	Т	Е		4	Т	Ч	С	Д

В результаті кінцевого зчитування по рядках повідомлення «ЗУСТРІЧАЙ У ДЕСЯТЬ» перетворялося у такий шифротекст: ЯІУУСРЗЙЬАТЕТЧСД. При розшифруванні порядок перестановок був зворотнім. Однак навіть шифри подвійної перестановки були слабким видом шифру, тому що легко читалися при будь-якому розмірі таблиці шифрування.

Новий етап розвитку криптології розпочався у другій половині XV століття з введенням у практику криптології багатоалфавітних шифрів заміни. Батьком цього шифру виявився теоретик мистецтва Леон Батіста Альберті (1404—1472), який узагальнив досвід гуманістичної науки у вивченні античної спадщини, написав трактати «Про статую», «Про живопис», «Про зодчество», десять книг про зодчество, побудував палац Ручеллаї, церкву Іль Джезу та ряд інших чудових здобутків зодчества середньовічної Італії.

У 1466 році Альберті надав до папської канцелярії також і трактат про шифри, де здійснив аналіз частот букв, дослідив шифри заміни та перестановки, торкнувся питань стійкості шифрів. Підмічена Альберті різночастотність появи букв в осмислених текстах дала поштовх вивченню синтаксичних властивостей письмових повідомлень. При цьому основна увага приділялась буквам, що частіше зустрічались у тексті.

Альберті вперше висунув ідею «подвійного» шифрування – текст, отриманий в результаті першого шифрування, піддавався повторному зашифруванню. Він запропонував використовувати два або більше шифралфавітів, переходячи від одного до іншого в процесі зашифровування й заплутуючи цим можливих криптоаналітиків.

Наприклад, обравши два шифралфавіти, можемо зашифрувати повідомлення, використовуючи по черзі то один, то інший. Таким чином, щоб зашифрувати слово *«UKRAINE»,* зашифруємо першу букву за допомогою першого шифроалфавіту, так що «*U*» перетвориться в «*Z*», другу ж букву ми зашифруємо, використовуючи другий шифралфавіт, при цьому *«K»* стане *«E».* Для зашифровування третьої букви ми повернемося знову до першого шифроалфавіту (*R* → *U*), а щоб зашифрувати четверту букву, ми знову звернемося до другого шифроалфавіту (*A* → *U*) і так далі: *I* → *M, N* → *H, E* → H. В результаті отримаємо такий шифротекст: *ZEUUMHH.*

Текст	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	X	Y	Z	W
Шифр 1	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	X	Y	Z	W	A	B	C
Шифр 2	U	X	Y	Z	W	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T

Основна перевага системи Альберті полягала в тому, що однакові букви у відкритому тексті не обов'язково залишалися однаковими у шифротексті. Точно так повторювані букви у шифротексті були різними буквами відкритого тексту.

В своїй книзі Альберті запропонував також свій власний шифр із нескромною назвою «шифр, гідний королів», який зробив шифровку дуже стійкою до «злому». Реалізація шифру забезпечувалась за допомогою механічного шифрувального диску, що було також одним з найважливіших винаходів Альберті.

Шифрувальний диск складався з великого зовнішнього диска та рухомого внутрішнього диска. Окружність зовнішнього диска була розділена на 24 рівні сектори, до яких були вписано 20 букв латинського алфавіту в їхньому природному порядку та 4 цифри. При цьому з алфавіту були вилучено 6 букв, без яких можна було обійтися – *H, J, K, U, Y, W.* Окружність внутрішнього диска була розділена також на 24 сектори, до яких були вписані букви змішаного латинського алфавіту.

Маючи два такі прилади, кореспонденти домовлялися про першу індексну букву на рухомому диску. При шифруванні повідомлення відправник ставив індексну букву проти будь-якої букви великого диска. Він інформував кореспондента про таке положення диска, записуючи цю букву зовнішнього диска як першу букву шифротекста. Чергова буква відкритого тексту відшукувалася на нерухомому диску, і буква меншого диска, що стояла проти неї, була результатом її шифрування. Після того, як були зашифровані декілька букв тексту, положення індексної букви змінювалося, про що також повідомлялося кореспонденту.

A B C D E F G I L M N O P Q R S T V X Z. 1…2 3. 4

L G A Z E N B O S F C H T Y. Q I. X K V P ET M R D

Так, наприклад, для індексної букви *«L»* одним з багатьох варіантів шифрування слова *«PRESIDENT»* може бути *«ATQEIOZECX»,* а іншим – *«BHYZQBAZFI»* тощо.

B C D E F G I L M N O P Q R S T V X Z 1. 2..3. 4 A

L G A Z E N B O S F C H. T Y Q I X K V P ET M R D

Такий шифр мав дві особливості, що робили винахід Альберті важливою подією в історії криптології. По-перше, на відміну від шифрів простої заміни шифродиск використовував не один, а декілька алфавітів для зашифрування. Такі шифри одержали назву багатоалфавітних. По-друге, шифродиск дозволяв використовувати так звані коди з перешифруванням, що

одержали широке поширення лише наприкінці XIX століття, тобто через чотири століття після винаходу Альберті.

Для цієї мети на зовнішньому диску малися цифри. Альберті склав код, що складався з 336 кодових груп, занумерованих від 11 до 4444. Кожному кодовому позначенню відповідала деяка закінчена фраза. Коли така фраза траплялася у відкритому повідомленні, вона замінялася відповідним кодовим позначенням, а за допомогою диска цифри зашифровувалися як звичайні знаки відкритого тексту, перетворюючись у букви.

У 1474 році був написаний перший у світі трактат, присвячений винятково криптоаналізу. Це зробив Чико Сімонетті, один із секретарів правителів Мілана – герцогів Сфорца. У ньому він виклав удосконалені шифри заміни, у тому числі шифр багатозначної заміни, у якому одній букві (голосній) відповідало декілька шифропозначень. Він розробив 13 правил розкриття шифрів простої заміни, у яких збережені роздільники слів. Рукопис, написаний на трьох шматках пергаменту, починався зі слів: «Перша необхідна умова полягає в з'ясуванні того, чи написаний документ латинською або місцевою мовою, а це можна установити в такий спосіб: з'ясуєте, чи мають слова в даному документі тільки п'ять різних закінчень, менше або більше. Якщо їх тільки п'ять або менше, ви праві, вважаючи, що документ написаний місцевою мовою…».

Сімонетті у своєму трактаті докладно описав шифри заміни, у яких для вирівнювання частоти появи букв у шифротексті голосним буквам ставився у відповідність не один знак, а декілька. Тут же вперше був наведений опис так званого «гаслового» шифру, що у різних модифікаціях буде застосовуватися й кілька століть пізніше. Правило заміни букв у ньому визначалося таким чином: під алфавітом писалася ключова фраза – гасло (наприклад, «*Ukraine*») без повторюваних букв, а потім букви, що у гаслі не зустрічалися, у природному порядку.

A B C D E F G H I. J. K L M N O P Q R S T U V W X Y Z
U K R A I N E B C D F G H. J. L M O P Q S T V W X Y Z

В результаті слово *«UZHGOROD»* перетворюється у шифротекст: *«TZBELPLA»*.

У 1518 році з'явилася перша друкована праця з криптології «Поліграфія» (лат. *Polygraphia).* Вона була написана Йоганом Гейденбергом (1462—1516), або Тритемієм (Трисемусом), абатом бенедиктинського монастиря Святого Мартіна (м. Вюрцбург, Німеччина), якого багато істориків вважають батьком європейської криптології. «Поліграфія» являла собою збірник з 6 книг і містила стовпці латинських термінів, слів, поставлених у відповідність буквам відкритого тексту, та першу квадратну таблицю, основу багатоалфавітної заміни.

Хоча у праці Тритемія було описано багато шифрів – як існуючих у той час, так і винайдених самим автором, вона була пронизана кабалістичними й окультними алюзіями.

В результаті книга викликала гнів багатьох монархових дворів Європи, які думали, що Тритемій видав у ній занадто багато таємниць. Крім того, Римська католицька церква вважала праці Тритемія єретичними та у 1609 році внесла його книги до списку заборонених. Ця заборона тривала 250 років.

У 1541 році книга була перевидана французькою мовою, а незабаром був зроблений її переклад на німецьку мову. У цій книзі Тритемій зробив дві нові пропозиції в криптології: він запропонував шифр «Аве Марія» і шифр, побудований на основі ключа, що періодично зрушується.

Шифр «Аве Марія» ґрунтувався на принципі заміни заздалегідь обговорених слів на букви шифротексту. З таких слів складалося зовні «безневинне» повідомлення. Наприклад, замінимо букви «А», «К», «Т» на такі слова: «А» – чекаю, мій; «К» – вдома, ключ; «Т» – я, тут. У такому разі позитивна таємна відповідь на задане питання може мати декілька варіантів: «Я чекаю вдома» або «Тут мій ключ».

Другим більш серйозним шифром була «таблиця Тритемія» – квадратна таблиця розміром 24х24 з багатьма алфавітами, яка була названа *«tabula recta»*. Алфавіти були записані в рядки таблиці один під іншим, причому кожний з них був зрушений на одну позицію вліво в порівнянні з попереднім.

Тритемій пропонував використовувати цю таблицю для багатоалфавітного шифрування найпростішим з можливих способів: перша буква тексту шифрувалася першим алфавітом, друга буква – другим тощо. У цій таблиці не було окремого алфавіту відкритого тексту, для цієї мети служив алфавіт першого рядка. Таким чином, слово *«UKRAINE»* перетворювалося у шифротекст *«ULTDNSL»*.

Перевага цього методу шифрування в порівнянні з методом Альберті полягала в тому, що кожна чергова буква текста шифрувалася новим алфавітом. Альберті змінював алфавіти лише після трьох або чотирьох слів. Тому його шифротекст складався з відрізків, кожний з яких мав закономірності відкритого тексту, що допомагали розкрити криптограму. Шифрування по буквах не давало такої переваги.

A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z
B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A
C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B
D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C
E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D
F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E
G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F
H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G
I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H
K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I
L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K
M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L
N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M
O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N
P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O
Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P
R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q
S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R
T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S
U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T
W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U
X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W
Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X
Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y

Крім того, Тритемій пропонував також використовувати одноалфавітне шифрування за допомогою квадрата Полібія та ключового слова – пароля. Обиралося яке-небудь слово, з нього прибиралися повторювані букви, а ті, що залишалися, записувалися в перші клітини квадрата. Порожні клітини заповнювалися буквами алфавіту, що залишилися, у природному порядку.

Розглянемо цю систему шифрування у варіанті для української мови, таблиця якої буде мати розмір не 5x5, а 5x6. Буква шифровки бралася з клітини, що знаходилася під клітиною букви повідомлення. Оскільки ключове слово легко було зберігати в пам'яті, то такий підхід спрощував процеси шифрування та дешифрування. Для ключа «ШИФРОВКА» таблиця буде мати такий вигляд (див. таблицю).

Ш	И	Ф	Р	О	В
К	А	Б	Г	Д	Е
Є	Ж	З	І	Л	М
Н	П	С	Т	У	Х
Ц	Ч	Щ	Ю	Я	Ь

Для вищеописаного шифру за даною таблицею повідомлення «УХОДИМО» дає шифровку «ЯЬДЛАХД». Такі табличні шифри були названі монограмними, тому що шифрування велося по одній букві.

Тритемій також першим помітив, що можна шифрувати одночасно по дві букви, які стояли разом та були названі «біграмою». Такий шифр був названий «біграмним». Опишемо його на прикладі тієї ж таблиці. Відкритий текст розбивався на біграми, а текст шифровки виходив з нього згідно з двома такими правилами:

1. Якщо обидві букви біграми вихідного тексту належали до одного стовпця таблиці, то буквами шифру вважалися букви, які були під ними. Так, біграма «РІ» давала текст шифровки «ГТ». Якщо буква відкритого тексту перебувала в нижньому рядку, то для шифру бралася відповідна буква з верхнього рядка: біграма «ЛЯ» давала шифр «УО» (біграма з однієї букви або пари однакових букв теж підкорялася цьому правилу).

2. Якщо обидві букви біграми вихідного тексту належали одному рядку таблиці, то буквами шифру вважалися букви, які лежали праворуч від них. Так, біграма «АД» давала текст шифровки «БЕ». Якщо буква відкритого тексту була в правому стовпці, то для шифру бралася відповідна буква з лівого стовпця: біграма «ІМ» давала шифр «ЛЄ».

3. Якщо обидві букви біграми відкритого тексту лежали в різних рядках і стовпцях, то замість них бралися дві букви таким чином, щоб вся їх четвірка складала прямокутник. При цьому послідовність букв у шифрі була віддзеркаленням вихідної пари. Наприклад, «АУ» шифрувалося як «ДП», а «ТБ» – як «СГ».

При шифруванні фрази «ОГОЛОШЕНИЙ ЗБІР» по біграмах виходить шифрування «РДДУВИКХААСЗТГ»:

ОГ ОЛ ОШ ЕН ИЙ ЗБ ІР

РД ДУ. ВИ. КХ АА. СЗ ТГ

Шифрування біграмами різко підсилило стійкість шифрів до розкриття.

При всьому тому, що «Поліграфія» була досить доступною друкованою книгою, описані в ній ідеї одержали визнання лише трьома століттями пізніше. Скоріше за все це було викликано непопулярністю Тритемія серед професійних криптологів, який був не криптологом, а богословом, бібліофілом і засновником архівної справи.

Наступний крок у розвитку запропонованого Тритеміем способа шифрування був зроблений італійцем Джовані Батіста Белазо. У 1553 році він опублікував брошуру «Шифр сеньйора Джовані Батіста Белазо» (італ. *La cifra del. Sig. Giovan Batista Belaso),* де запропонував використовувати для багатоалфавітного шифру буквений ключ, що був названий ним «паролем» та повинен був легко запам'ятовуватися. Пароль виписувався під або над рядком повідомлення. Буква пароля, що знаходилися над (під) буквою повідомлення, визначала номер рядка таблиці Тритемія, тобто алфавіт заміни, згідно з яким і здійснювалося шифрування. Буква повідомлення визначала номер стовпця таблиці, а буква шифротекста знаходилась на перетинанні рядка та стовпця таблиці.

Приблизно в той же час італійський математик і філософ Джироламо Кардано (1501—1576) запропонував використовувати як ключ сам текст повідомлення, тобто «самоключ» або «автоключ» (autokey). Наприклад, у фразі «ЗБІР СЬОГОДНІ» ключем було слово «ЗБІР»:

текст – ЗБІРСЬОГОДНІ

ключ – ЗБІР ЗБІР ЗБІР

Шифрування здійснювалось за допомогою таблиці Тритемія.

Крім того, у 1556 році захоплення теорією магічних квадратів привело Кар-дано до відкриття нового класу шифру перестановок, названого ґратами або трафаретом. Вони являли собою квадратні таблиці, де чверть осередків прорізана так, що при чотирьох поворотах вони покривали весь квадрат. Вписування в прорізані осередки тексту й повороти ґрат тривали доти, поки весь квадрат не був заповнений. Наприклад, на малюнку нижче показаний процес шифрування ґратами 4х4. Трафарет мав 4 прорізані клітини, а повороти здійснювалися за годинною стрілкою на зазначений нижче кут (див. таблицю).

Трафарет		0°		90°
■ ■ □ ■	→	□ □ З □	→	Р □ □ □
■ ■ ■ □		□ □ □ У		□ І □ □
■ □ ■ ■		□ С □ □		□ □ □ Ч
□ ■ ■ ■		Т □ □ □		□ □ А □

180°		270°		Шифровка
□ □ □ Й	→	□ С □ □	→	Р С З Й
□ □ У □		Я □ □ □		Я І У У
□ □ □ □		□ □ Т □		Д С Т Ч
□ Е □ □		□ □ □ Ь		Т Е А Ь

Головна вимога до ґрат – при усіх поворотах «вікна» не повинні попадати на одне й те місце у квадраті, у якому утвориться шифротекст. Якщо у квадраті після зняття ґрат утворювалися пусті місця, то в них вписувалися будь-які букви.

Кількість подібних ґрат швидко росте з їхнім розміром. Так, ґрати 2х2 єдині, ґрат 4х4 уже 256, а ґрат 6х6 понад сто тисяч. Незважаючи на певну складність, шифри типу ґрат досить просто розкривалися, тому не могли використовуватися як самостійний шифр. Однак вони були дуже зручними та ще довго використовувалися в практиці для посилення шифрів заміни.

Воскресити змішані алфавіти, що застосовував Альберті, та об'єднати ідеї Альберті з ідеями Тритемія і Белазо в сучасну концепцію багатоалфавітної заміни випало на долю італійця Джовані Батіста дела Порта (1535—1615). Йому було 28 років, коли він у 1563 році опублікував книгу «Про приховану значущість окремих букв» (лат. *De Furtivis Literarum Notis).* її перші два розділи були присвячені криптографії, а в інших двох викладалися основи криптоаналізу та розглядалися лінгвістичні особливості, що допомагали розкриттю шифрів.

Книга Порти містила перший в Європі опис того, як варто розкривати шифр простої заміни, коли шифротекст не був розділений на слова або був розділений неправильно. Порта також описав те, що вважалося другим за значимістю прийомом у сучасному криптоаналізі:

«…Коли тема листування відома, дослідник може зробити проникливі припущення щодо слів, що звичайно вживаються в такому контексті. Ці слова можна без великої праці знайти, помічаючи в текстах кількість знаків, а також подібність і розходження букв… Для кожної теми характерні деякі загальні слова, що супроводжують її, будучи необхідними. Наприклад, у любові – це «пристрасть», «серце», «вогонь», «полум'я», «згоряти», «життя», «смерть», «жалість», «жорстокість»; на війні – «солдат», «командир», «генерал», табір», «зброя», «боротися» і т. д. Таким чином, цей прийом розкриття, що не заснований на аналізі самих документів або на спробі розбити текст на голосні або приголосні, може полегшити задачу».

У своїй книзі Порта також дав одну мудру пораду, що й сьогодні корисна криптоаналітику такою ж мірою, якою вона була доречна в Італії епохи Відродження:

«Необхідні повна зосередженість і ретельність, щоб вільна від сторонніх думок голова, коли все інше відкладено убік, була цілком зайнята єдиною задачею доведення початої справи до успішного завершення. І все-таки, коли така задача вимагає надмірного напруження і незвичайних витрат часу, напруження не повинно бути безперервним, не слід навантажувати мозок надмірно, тому що занадто великі зусилля і тривале розумове навантаження призводять до нервового виснаження, після якого голова вже менш придатна для подібних речей та з неї вже не вичавиш нічого…»

А далі Порта поділився з читачем своїм власним практичним досвідом роботи: «Крім того, дуже важливо, щоб повідомлення було написано рукою автора або митецького переписувача, тому що якщо перехоплене повідомлення буде скопійовано неправильно або якщо воно вийде з-під руки людини, незнайомого з мистецтвом шифру, то в результаті, оскільки правопис порушений, будь-яка інтерпретація повідомлення буде блокована».

Подібний досвід приходив тільки до криптоаналітика, що мав справу з повідомленнями, у яких букви часто були пропущені, переставлені або замінені на інші. Це траплялося лише при обробці дійсних криптограм. Завдання, що зустрічалися в книгах з криптоаналізу того часу, завжди були бездоганно складені з точки зору правопису й тому легко вирішувалися. Скоріше за все, Порта регулярно займався криптоаналізом, виконуючи доручення папської курії.

Повною мірою чудові здібності Порти проявилися при рішенні найбільш важкої проблеми криптоаналізу епохи Відродження – розкритті багатоалфавітних шифрів. Незважаючи на високу оцінку цих шифрів криптоаналітиками того часу, Порта відмовився визнати їхню невразливість і розробив для них методи розкриття. Хоча ці методи не були універсальними, їхня основна цінність складалася в застосованому Портою сміливому підході, що й привів його до успіху.

Для початку Порта спробував прочитати шифротекст, який його сучасниками був зашифрований за допомогою спеціального приладу. Цей прилад складався з двох дисків: внутрішнього нерухомого диска, на який за годинною стрілкою був нанесений алфавіт відкритого тексту, і зовнішнього рухливого диска з низкою вигадливих шифрознаків. Зовнішній диск після зашифрування чергової букви повертався за годинною стрілкою на один крок. Порта помітив, що якщо в якому-небудь слові відкритого тексту три букви підряд стояли в алфавітній послідовності, той самий шифрознак 3-разово повторювався у шифротексті. Це допомогло йому прочитати криптограму.

Потім Порта модифікував розроблений ним метод, щоб дешифрувати іншу багатоалфавітну криптограму, яка була складена згідно з принципом Джовані Белазо. На думку Порти, у криптограмі 3-кратне повторення букви шифротекста сигналізувало про те, що ключем із трьох букв, розташованих в звичайному алфавітному порядку, був зашифрований відкритий текст, у якому було три букви в порядку, протилежному алфавітному. Міркуючи з цього при-

воду, Порта впритул підійшов до універсального методу розкриття багатоалфавітних шифрів, знайти який він так прагнув:

«Оскільки… між першими трьома „М“ і цими ж трьома буквами, повтореними в 13-му слові, знаходиться 51 буква, я дійду висновку, що ключ повторений три рази, і правильно вважаю, що він містить 17 букв».

Однак Порта так і не скористувався своїм спостереженням. У результаті багатоалфавітний шифр продовжував вважатися надійним протягом трьох наступних століть.

У своїй книзі Порта ввів свою таблицю багатоалфавітного шифрування (див. таблицю).

A	A	B	C	D	E	F	G	H	I	K	L	M
B	N	O	P	Q	R	S	T	U	W	X	Y	Z
C	A	B	C	D	E	F	G	H	I	K	L	M
D	O	P	Q	R	S	T	U	W	X	Y	Z	N
E	A	B	C	D	E	F	G	H	I	K	L	M
F	P	Q	R	S	T	U	W	X	Y	Z	N	O
G	A	B	C	D	E	F	G	H	I	K	L	M
H	Q	R	S	T	U	W	X	Y	Z	N	O	P
I	A	B	C	D	E	F	G	H	I	K	L	M
K	R	S	T	U	W	X	Y	Z	N	O	P	Q
L	A	B	C	D	E	F	G	H	I	K	L	M
M	S	T	U	W	X	Y	Z	N	O	P	Q	R
N	A	B	C	D	E	F	G	H	I	K	L	M
O	T	U	W	X	Y	Z	N	O	P	Q	R	S
P	A	B	C	D	E	F	G	H	I	K	L	M
Q	U	W	X	Y	Z	N	O	P	Q	R	S	T
R	A	B	C	D	E	F	G	H	I	K	L	M
S	W	X	Y	Z	N	O	P	Q	R	S	T	U
T	A	B	C	D	E	F	G	H	I	K	L	M
U	X	Y	Z	N	O	P	Q	R	S	T	U	W
W	A	B	C	D	E	F	G	H	I	K	L	M
X	Y	Z	N	O	P	Q	R	S	T	U	W	X
Y	A	B	C	D	E	F	G	H	I	K	L	M
Z	Z	N	O	P	Q	R	S	T	U	W	X	Y

Шифрування повідомлення здійснювалося за допомогою секретного гасла-пароля, що періодично виписувався над відкритим текстом. Буква гасла визначала алфавіт (заголовні

букви першого стовпця), розташована під ключем буква відкритого тексту шукалася у верхньому або нижньому напівалфавіті та замінялася відповідною їй буквою другого напівалфавіту.

Наприклад, якщо як гасло використати слово «*UKRAINE*», то шифрування слова «*UZHGOROD*» буде виглядати таким чином:

гасло .....UKRAINE
відкритий текст …UZHGOROD
шифротекст ……LHQTKLMN

За цей шифр Порту пізніше назвали батьком сучасної криптографії, але у той час цей шифр не знайшов широкого застосування. Причиною цього була необхідність постійно мати при собі вказану таблицю та складність процесу шифрування. Разом з тим, був даний імпульс для появи інших шифрувальних систем (наприклад, Віженера).

Також Порта запропонував шифр простої біграмної заміни з використанням квадратної таблиці зі змішаним алфавітом і паролем. У ньому пари букв (біграми) позначалися одним спеціальними графічними символами. Наприклад, біграма «*EA*» замінялася грецьким символом «*Δ*», біграма «*LF*» – символом «*Ψ*» тощо.

Вони заповнювали квадратну таблицю розміром 20х20, рядки й стовпці якої були занумеровані буквами латинського алфавіту. По суті справи це був той же шифр простої заміни, але на рівні двобуквених сполучень. Криптостійкість при такій заміні порівняно до шифрування по буквах значно підвищувалась.

Французький посол у Римі Блез де Віженер (1523—1596), ознайомившись з криптологічними працями та ідеями Цезаря, Альберті, Тритемія, Белазо й Порта, захопився криптологією. У 1585 році він написав книгу «Трактат про шифри» (фр. *Traite des chiffres),* де виклав основи криптології. В ній він висловив думку про те, що «усі речі у світі являють собою шифр. Уся природа є просто шифром і таємним листом». Пізніше цю думку повторили і Блез Паскаль, і батько кібернетики Норберт Вінер.

У своєму трактаті Віженер знову повторив ідею Кардано щодо використання «самоключа». Заздалегідь обмовлялася одна ключова буква алфавіта, та перша буква повідомлення шифрувалася за рядком таблиці Тритемія, що відповідав цій букві. Друга буква повідомлення шифрувалась за рядком, що відповідав першій букві шифротексту і так далі.

Другий варіант використання таблиці Тритемія, запропонований Віженером, полягав у застосуванні ключа-гасла. По суті Віженер, об'єднавши підходи Тритемія, Белазо, Порта до шифрування відкритих текстів, не вніс у них нічого оригінального.

Шифр Віженера містив у собі алфавітну квадратну таблицю Тритемія, що складалася з 24 покрокових ротацій у лівий бік прямого стандартного латинського алфавіту. У цій таблиці перший горизонтальний рядок називався «лінією мови», а перший вертикальний стовпчик ліворуч – «таємною лінією». Ключем могло бути будь-яке слово, букви якого виписувалися підряд над чи під буквами відкритого листа. Причому, коли воно закінчувалось, то записувалося знову, циклічно повторюючись, поки не закінчувався текст.

Цей ключ і був «таємницею», який Белазо називав «паролем», а Віженер назвав «гаслом». У наш час ключова послідовність букв або цифр одержала назву «гама» за аналогією з відомим музичним терміном. Таблиця Віженера легко відновлювалася перед самим процесом шифрування, після чого могла бути знищена.

Запропонована Віженером шифросистема стала першим великим відкриттям у криптології з часів Юлія Цезаря, яка протягом 350 років вважалася однією з найнадійніших систем. Головною її перевагою була простота.

	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z
B	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A
C	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B
D	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C
E	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D
F	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E
G	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F
H	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G
I	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H
K	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I
L	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K
M	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L
N	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M
O	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N
P	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O
Q	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P
R	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q
S	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R
T	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S
U	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U
X	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X
Z	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y

Повідомлення шифрувалося буква за буквою, для чого в таблиці треба було знайти стовпець, позначений тією ж буквою, що й відповідна буква ключа, та рядок, позначений тією же буквою, що й буква відкритого тексту, що лежала під даною буквою ключа. Буква, що лежала у таблиці на перетинанні зазначених стовпця та рядка, й була потрібним шифросимволом.

Наприклад, якщо як ключ використати слово *«UKRAINE»,* то шифрування слова *«UZHGOROD»* виглядатиме таким чином:

відкритий текст …UZHGOROD

ключ .....UKRAINEU

шифротекст ……PHWGYESZ

Шифр Віженера мав також деякі з переваг більш раннього номенклаторного типу шифру. Кожна буква відкритого тексту могла передаватися в шифротексті таким числом різних шифросимволів, скільки різних букв утримувалося в ключі. Крім того, багатоалфавітна заміна дозволяла приховувати повторювані букви й інші внутрішньословні сполучення, характерні для даного відкритого тексту. При цьому в остаточному шифротексті використовувалися тільки 24 звичайні букви алфавіту, а які-небудь спеціальні символи або цифри були не потрібні.

Астрологічні захоплення Віженера привели його до шифру, у якому шифрознаками були положення небесних тіл у момент шифрування. Він спробував перевести свої послання на «мову неба».

У XIX сторіччі британський адмірал сер Френсіс Бофорт (1774—1857) запропонував свій різновид шифру Віженера – шифр (квадрат) Бофорта (Бьюфорта). Його рядками були рядки квадрата Віженера, але записані в зворотньому (зеркальному) порядку (див. таблицю).

	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z
A	Z	Y	X	W	U	T	S	R	Q	P	O	N	M	L	K	I	H	G	F	E	D	C	B	A
B	Y	X	W	U	T	S	R	Q	P	O	N	M	L	K	I	H	G	F	E	D	C	B	A	Z
C	X	W	U	T	S	R	Q	P	O	N	M	L	K	I	H	G	F	E	D	C	B	A	Z	Y
D	W	U	T	S	R	Q	P	O	N	M	L	K	I	H	G	F	E	D	C	B	A	Z	Y	X
E	U	T	S	R	Q	P	O	N	M	L	K	I	H	G	F	E	D	C	B	A	Z	Y	X	W
F	T	S	R	Q	P	O	N	M	L	K	I	H	G	F	E	D	C	B	A	Z	Y	X	W	U
G	S	R	Q	P	O	N	M	L	K	I	H	G	F	E	D	C	B	A	Z	Y	X	W	U	T
H	R	Q	P	O	N	M	L	K	I	H	G	F	E	D	C	B	A	Z	Y	X	W	U	T	S
I	Q	P	O	N	M	L	K	I	H	G	F	E	D	C	B	A	Z	Y	X	W	U	T	S	R
K	P	O	N	M	L	K	I	H	G	F	E	D	C	B	A	Z	Y	X	W	U	T	S	R	Q
L	O	N	M	L	K	I	H	G	F	E	D	C	B	A	Z	Y	X	W	U	T	S	R	Q	P
M	N	M	L	K	I	H	G	F	E	D	C	B	A	Z	Y	X	W	U	T	S	R	Q	P	O
N	M	L	K	I	H	G	F	E	D	C	B	A	Z	Y	X	W	U	T	S	R	Q	P	O	N
O	L	K	I	H	G	F	E	D	C	B	A	Z	Y	X	W	U	T	S	R	Q	P	O	N	M
P	K	I	H	G	F	E	D	C	B	A	Z	Y	X	W	U	T	S	R	Q	P	O	N	M	L
Q	I	H	G	F	E	D	C	B	A	Z	Y	X	W	U	T	S	R	Q	P	O	N	M	L	K
R	H	G	F	E	D	C	B	A	Z	Y	X	W	U	T	S	R	Q	P	O	N	M	L	K	I
S	G	F	E	D	C	B	A	Z	Y	X	W	U	T	S	R	Q	P	O	N	M	L	K	I	H
T	F	E	D	C	B	A	Z	Y	X	W	U	T	S	R	Q	P	O	N	M	L	K	I	H	G
U	E	D	C	B	A	Z	Y	X	W	U	T	S	R	Q	P	O	N	M	L	K	I	H	G	F
W	D	C	B	A	Z	Y	X	W	U	T	S	R	Q	P	O	N	M	L	K	I	H	G	F	E
X	C	B	A	Z	Y	X	W	U	T	S	R	Q	P	O	N	M	L	K	I	H	G	F	E	D
Y	B	A	Z	Y	X	W	U	T	S	R	Q	P	O	N	M	L	K	I	H	G	F	E	D	C
Z	A	Z	Y	X	W	U	T	S	R	Q	P	O	N	M	L	K	I	H	G	F	E	D	C	B

Ця таблиця мала одну перевагу – правила зашифрування та розшифрування були однакові: і в тому, і в іншому випадку букви, що шифрувалися та дешифрувалися, витягалися з верхнього алфавітного рядка.

Заради історичної справедливості необхідно зазначити, що таблиця Бофора була запропонована ще у XVIII сторіччі італійцем Дж. Сестрі. Однак його ім'я в історії виявилося забутим.

Людиною, що зуміла зробити криптологію окремою науковою дисципліною, став англійський філософ і державний діяч Френсіс Бекон (1561—1626), який був одним з розумніших людей свого часу та автором більше, ніж двох десятків робіт, опублікованих та визнаних сучасниками ще при його житті. Будучи лордом-канцлером при королі Якові I, він добре знав потреби держави в надійних шифрах, тому його перша талановита робота, що відносилася до 1580 року, надалі одержала блискучий практичний розвиток.

Присвятивши криптології спеціальні роботи «Успіх пізнання» та «Про достоїнство і збільшення наук», він був не тільки теоретиком, але й мистецьки застосовував на практиці свої знання, завдяки чому зайняв почесне місце серед видатних європейських криптологів. Зокрема, саме він уперше запропонував свою систему тайнопису, назвавши її «двобуквеним» шифром. Практично це було «двійкове кодування» букв латинського алфавіту – те ж саме, яке використовується зараз у комп'ютерах (див. таблицю).

a	AAAAA	g	AABBA	n	ABBAA	t	BAABA
b	AAABA	h	AABBB	o	ABBAB	u,v	BAABB
c	AAABB	i,j	ABAAA	P	ABBBA	w	BABAA
d	AAABB	k	ABAAB	q	ABBBB	x	BABAB
e	AABAA	l	ABABA	r	BAAAA	y	BABBA
f	AABAB	m	ABABB	s	BAAAB	z	BABBB

По суті, це була бінарна система стеганографії, оскільки за допомогою шрифтів двох видів (наприклад, «*A*» і «*B*») у букви довільного (нетаємного) тексту потай вносилася додаткова (таємна) інформація. Кожній букві таємного послання ставилося у відповідність п'ять букв звичайного відкритого тексту.

На початку XVII століття Матео Ардженті, криптолог папської канцелярії, склав посібник з криптології на 135 аркушах, що був виданий у плетінні з телячої шкіри. У цій книзі він повторив ідею Чико Сімонетті щодо використання деякого слова як ключа для отримання змішаного алфавіту. Наприклад, ключове слово «*UKRAINE*» дає такий змішаний латинський алфавіт:

U K R A I N E B C D F G H J L M O P Q S T V W X Y Z

Такі змішані алфавіти часто використовувалися як алфавіти шифротексту в шифрах простої заміни. З метою ускладнення шифру простої заміни Ардженті рекомендував не розділяти слова, використовувати «омофонні» заміни, вставляти у шифротекст велику кількість «пустишок» (Ø), усувати пунктуацію, не вставляти у шифротекст відкриті слова («клер») тощо. Для букв, що часто траплялися у словах, він ввів декілька позначень, а для сполучень букв, що часто траплялися у текстах, – окремі позначення. Пізніше подібні ідеї одержали широке поширення.

Приведемо приклад шифру Ардженті:

A. B.. C.. D.. …E…..F.. G.. H.. I. L.. M. N..O. P

1 86 02 20 62,82 22 06 60 3 24 26 84 9 66

Q…R…S… T.. …U…..Z. ET CON NON CHE ~~Ø~~

68 28 42 80 04,40 88 08.. 64.. 00… 44.. 5,7

Слово *«UZHGOROD»* може бути зашифровано багатьма способами, наприклад: 0488600659289720 або 754078856070692859205577.

Найбільшим досягненням Ардженті вважається розроблений ним буквений код (номенклатор), у якому 1200 букв, складів, слів та цілих фраз замінялися групами букв.

У XVII столітті найбільш цінною історичною працею в сфері криптології були твори Густава Селена (псевдонім Августа II герцога Брауншвейг-Люнебурга, князя Брауншвейг-Вольфенбюттеля) (1579—1666) «Криптописьмо і криптографія» (лат. *Cryptomenytices et cryptographie):* «Дев'ять книг Густава Селена, у яких викладається навчання про приховання змісту і тайнопису, написане Йоганом Тритемієм, настоятелем у Спенхеймі і Хербиполені, чоловіка чудесного розуму і схованих магічних здібностей. Тут же викладені важливі способи й інших авторів. 1624 р.». Ці книги, до речі, були навчальними посібниками російського криптолога XVIII століття Епінуса.

Криптологія вже була відома багатьом та застосовувалася в багатьох шарах суспільства. Так, англієць Самуель Пепіс (1633—1703) став всесвітньо відомим своїм зашифрованим щоденником, згідно з яким історики пишуть праці про перехід від Пуританства до Реставрації. Мистецтвознавці включили цей добуток у світову скарбницю літератури. Пепіс закінчив Кембридж завдяки кузену батька – адміралу Монтегю та мав багато друзів: ученого Ісаака Нью-

тона, архітектора Крістофера Рена, поета й драматурга Джона Драйдена. Пепіс був особисто свідком таких незабутніх для Англії подій, як повернення короля Чарльза II в Англію, велика чума 1664 року, пожежа Лондона 1666 року, революція 1688 року.

Свої мемуари Пепіс зашифрував за системою криптолога Томаса Шелтона та додатково своїм власним шифром, оскільки містили багато скандальних фактів про великих сучасників. Разом з його особистими книгами та паперами щоденник після смерті письменника потрапив у Кембридж, де відразу ж привернув увагу дослідників. Перший успіх у його розшифруванні був отриманий лише в 1822 році, а повністю він був розшифрований у 1899 році.

3. Ера «чорних кабінетів»

У 1506 році «секретарем з шифрів» Венеціанської республіки був призначений Джованні Соро. Він прославився тим, що з успіхом розкривав шифри численних європейських князівств. Слава Соро була настільки велика, що починаючи з 1510 року папська курія надсилала йому для розкриття шифри, з якими не могли справитися в Римі. У 1526 році папа Климент VII двічі направляв Соро перехоплені депеші для дешифрування, і обидва рази Соро домігся успіху. А коли одне з послань Климента потрапило в руки його супротивників, той викрикнув: «Соро може розкрити будь-який шифр!», – і направив Соро копію цього послання, щоб з'ясувати, чи надійно воно зашифровано. Климент заспокоївся тільки тоді, коли Соро повідомив, що не може його прочитати. Хоча хто знає, чи не намагався Соро навмисно ввести папу в оману помилковими заявами про надійність його шифру.

У 1542 році Соро отримав двох помічників. З цього часу Венеція мала вже трьох кваліфікованих криптоаналітиків. їхнє приміщення знаходилося в палаці венеціанського правителя, де вони працювали за зачиненими дверима. Нікому не дозволялось їх турбувати, а їм самим не дозволялося залишати своє робоче приміщення, поки не буде знайдений відкритий текст чергової перехопленої криптограми. Криптоаналітики Венеції також писали трактати, у яких роз'яснювали методи своєї роботи. Праця Соро про дешифрування листування на латинській, італійській, іспанській та французькій мовах, написана ним на початку XVI століття, на жаль, була загублена. Але вціліли уривчасті записи його спадкоємця, а також дослідження в цій сфері інших венеціанських секретарів із шифрів.

Джованні Соро став першим, хто почав готувати професійні кадри для криптології, і хоча це була досить примітивна форма «учнівства», позбавлена достатньої теоретичної бази, вона була переважною протягом тривалого часу. Справа в тому, що люди, які працювали з шифрами того часу, були добре освічені, але успішно освоїти криптологічну справу, яка постійно еволюціонувала й ускладнювалася, можна було тільки за допомогою довгої практики, чим і займався Соро зі своїми учнями.

Спеціальних навчальних закладів, де навчали б криптологічної діяльності в той час не існувало. Криптологів рекрутували з найбільш освічених людей того часу, що знали математику й іноземні мови. Соро був першим, хто спробував спеціально навчати молодих криптологів цій науці, але знову ж на практиці. З іншої боку, сама проблема кадрів не стояла в той час так гостро, а посада секретаря з шифрів була досить бажаною для багатьох обдарованих людей того часу, тому що давала славу, повагу й чималий матеріальний прибуток.

Багато видатних математиків, починаючи з тих часів, залучалися до крипто-логічних служб. Папи Римські завжди користувалися послугами криптологів, тому видатний італійський математик і філософ Джироламо Кардано в середині XVI століття перебував у них на службі, а також був і астрологом. Крім того, він винайшов шарнірний механізм та метод вирішення рівнянь третього ступеня, а у 1550 році опублікував книгу «*De subtilitate libri xxi*».

Римський Папа Павло III, що змінив Клімента VII, швидко зрозумів, що не в його інтересах посилати шифри для розкриття за кордон. У 1555 році в папській курії була заснована посада секретаря з шифрів. Перший успіх прийшов тільки через два роки, коли папські криптоаналітики розкрили шифр іспанського короля Пилипа II, що тоді воював з Папою Римським. А в 1567 році відзначився вікарій собору Святого Петра в Римі, який менше, ніж за шість годин зумів прочитати криптограму, написану турецькою мовою, на якому вікарій не знав і чотирьох слів.

У Флоренції Піро Музефілі, граф Сасетський, з 1546 по 1557 роки прочитав безліч шифрованих повідомлень, розкривши серед інших номенклатори, що використовувалися в листуванні між французьким королем Генріхом II і його послом у Данії. Криптоаналітична екс-

пертиза Музефілі була настільки кваліфікованою, що багато хто приїжджали до нього, як і до Соро, з проханням розкрити для них шифри. Серед клієнтів Музефілі був і король Англії, який надіслав йому криптограму, що була знайдена в підметках туфель, доставлених до його двору з Франції.

У XVI столітті не тільки італійські правителі славилися своїми криптоаналітиками. У Франції в дешифруванні перехоплених депеш найбільше процвітав Филібер Бабу (1484—1557), який був першим державним секретарем і казначеєм короля Франциска I. Один спостерігач описував, як Бабу, «не маючи алфавіту, часто дешифровував багато перехоплених депеш на іспанській, італійській та німецькій мовах, хоча він не знав жодної з цих мов або знав дуже погано, причому він завзято працював над повідомленням дні і ночі безперервно протягом трьох тижнів, перш ніж розгадував одне слово. Після того, як пролом був пророблений, інше відбувалося дуже швидко та нагадувало руйнування стін». Варто помітити, що в той час, як Бабу не покладаючи рук працював на короля, король приймав у себе коханку – чарівну дружину Бабу. Бабу одержав багато милостей від короля, але важко сказати, за що саме: за криптоаналітичні успіхи чи за дозвіл наставляти «роги».

У Голландії також працював блискучий криптоаналітик – фламандський дворянин Пилип ван Марнікс, барон де Сент-Альдегонд (1538—1598), автор мелодії сучасного національного гімну Голландії, права рука Вільгельма Оранського, що стояв на чолі об'єднаного повстання голландців і фламандців проти Іспанії. В 1577 році Голландією керував іспанський губернатор дон Хуан Австрійський, рідний брат іспанського короля Пилипа II. Його метою було скинення з трону королеви Англії Єлизавети, захоплення англійської корони та одруження з чарівною королевою Шотландії Марією Стюарт. Однак у червні того ж року у Франції були перехоплені шифровані листи дона Хуана.

Вони були переправлені Марніксу, який через місяць розкрив іспанський шифр. Після цього зміст листів через Вільгельма Оранського був доведений до відома міністра Єлизавети Френсіса Уолсінгема. Уолсінгем одразу ж здійснив заходи щодо отримання більш повної інформації та незалежності від іноземних криптоаналітиків. З цією метою він направив до Парижа талановитого юнака, який швидко розправлявся з шифрованими листами. Це був Томас Феліпес, перший видатний криптоаналітик з Англії.

За результатами проведених заходів все шифроване листування Марії Стюарт, в якому вона давала згоду на змову проти Єлизавети та рекомендації! щодо її здійснення, розшифровувалося Феліпесом та надходило до Уолсингема. Ці листи та шифр, яким вона користувалася разом з іншими зрадниками, послужили головним матеріалом для обвинувачення на засіданнях суду, який визнав Марію Стюарт винною у державній зраді. 8 лютого 1587 року о 8-й годині ранку вона піднялась на ешафот, стала на коліна та мужньо прийняла від ката три удари сокирою. Таким чином, криптоаналіз прискорив смерть Марії, королеви Шотландії.

У 1589 році королем Франції став Генріх IV, що відразу ж був змушений вступити в запеклу боротьбу зі Священною лігою. Священна ліга на чолі з герцогом Майенським контролювала столицю та всі інші великі міста Франції, одержуючи великі підкріплення у вигляді живої сили та грошей від іспанського короля Пилипа II. Генріх був з усіх боків оточений супротивником. Але саме в цей важкий для нього час у його руки потрапила частина листування Пилипа з іспанським воєначальником Хуаном Моро.

Листи Пилипа були зашифровані, але в Генріха секретарем з шифрів у той час служив 49-літній математик Франсуа Вієт (1540—1603), засновник сучасної елементарної алгебри. Його теорему про коріння й коефіцієнти квадратних рівнянь дотепер вивчають у школі. Він також був членом таємної ради та займався адвокатською практикою. У 1588 році Вієт прочитав шифровану іспанську депешу, адресовану Олесандро Фарнезе, герцогу Парми, що командував іспанськими військами Священної ліги.

З тих пір Генріх передавав Вієту всі нові перехоплені депеші, щоб з'ясувати, чи зможе той повторити свій успіх. Вієт, працюючи разом з голландським криптоаналітиком Пилипом ван Марніксом, зумів приблизно за рік розкрити шифр короля Іспанії Пилипа II, що до цього часу вважали невразливим не тільки в Іспанії, але й у Ватикані – одному з найбільших криптологічних центрів того часу.

Розвиток криптоаналізу на Заході виявився в прямій залежності від розквіту дипломатії. З тих пір, як держави стали підтримувати постійні дипломатичні відносини, їхні посли, яких іноді іронічно називали «почесними шпигунами», регулярно відправляли до себе на батьківщину великі послання. Існуючі між державами суперництво й підозрілість змушували дипломатів зашифровувати свої депеші, оскільки їх нерідко перехоплювали та розкривали.

Поява постійних дипломатичних представництв та загострення політичної боротьби стимулювало послів зашифровувати свої повідомлення, побоюючись, що вони будуть перехоплені супротивником. До кінця XVI сторіччя криптоаналіз став грати настільки важливу роль, що в більшості європейських держав були введені посади секретарів з шифрів, які повний робочий день займалися шифруванням і розшифруванням своїх повідомлень, а також дешифруванням перехоплених депеш.

XVII століття ввійшло в історію криптоаналізу як ера *«cabinets noirs»,* або «чорних кабінетів» (далі – ЧК). У цей час у різних країнах почали з'являтися перші служби перлюстрації (лат. *perlustro* – оглядаю) та дешифрування «розкритої» кореспонденції, які розташовувались у секретних кімнатах.

У серпні 1620 року голландський посол в Англії Жан Баптист Ван Мале старанно намагався підкупити урядового шифрувальника Вінсентіо, який ще до цього відсидів 6 років у Тауері за зв'язки з іспанською розвідкою. Ван Мале хотів спонукати Вінсентіо відмовитися розшифровувати важливі листи іспанського посла у Відні до голландського правителя ерцгерцога Альберта, перехоплені англійськими розвідниками. Вінсентіо пропонувалися гроші – зрозуміло, з прямо протилежною метою – також і від імені голландського посла. Всі договірні сторони торгувалися при цьому, як на ринку. А тим часом англійські власті спохопилися та запропонували Вінсентіо поквапитися з розшифровкою, якщо він не бажає познайомитися з камерою катування…

В той же час іспанський посол в Англії Гондомар дізнався, що англійці читають його листи, які він направляв до Мадрида. Там копії з них якимсь невідомим шляхом здобував англійський посол сер Джон Дігбі, розшифровував місця, написані кодом, і пересилав свою здобич до Лондона Якову I. Марно Гондомар міняв шифри і кур'єрів, просив, щоб в Мадриді його донесення потрапляли тільки до рук абсолютно довірених осіб. Тільки через багато років, вже повернувшись з Іспанії, Дігбі, поступаючись наполегливим проханням Гондомара, розповів, що депеші перехоплювалися і копіювалися, поки кур'єр відпочивав на останній поштовій станції недалеко від іспанської столиці.

Взагалі ж, у XVI—XVII століттях криптослужби з'явилися практично в кожній європейській державі, причому до складу цих служб входила наукова еліта того часу: Франсуа Вієт і Антуан Россиньоль у Франції, Джироламо Кардано в Римі, Джон Валліс і Френсіс Бекон в Англії, Вільгельм Лейбніц у Німеччині. Європейські правителі нерідко залучали вже відомих криптологів-іноземців на службу, хоча це не завжди вдавалося. Мабуть, самим неуспішним із таких криптологів був Готфрід Вільгельм Лейбніц (1646—1716) – видатний німецький учений, математик, засновник Берлінської академії наук.

Англійський король Георг I хотів запросити Лейбніца, щоб той очолив британську криптослужбу, але натрапив на різку протидію в особі Джона Валліса (1616—1703), який побоювався конкуренції з боку свого німецького колеги та пригрозив королю перейти на бік Іспанії, видавши їй всі англійські секрети, яких Валліс за характером своєї діяльності знав чимало.

Активно виступав проти подібного призначення й Ісаак Ньютон (1642—1727) – голова Королівського наукового суспільства, який заперечував авторство Лейбніца у диференційному обчисленні. Не поталанило Лейбніцу й іншого разу, коли його запросив до Росії Петро I не тільки для організації Російської академії наук, але й для створення російської криптослужби за європейським зразком. Смерть Лейбніца не дозволила здійснитися планам Петра, змушеного скористатися послугами менш іменитих криптологів.

В Англії лорд-протектор Олівер Кромвель створив «Інтелідженс сервіс» (англ. *Intelligence service* – служба розвідки), до складу якої входив підрозділ із дешифрування. Його очолював відомий математик Джон Валліс (Уолліс), який володів унікальними здібностями. Так, безсонними ночами він вираховував квадратний корінь із 50-значних чисел з точністю до 20-30-го знаків.

Англійський король Карл II цінував мистецтво Валліса та називав його «дорогоцінним каменем для короля…». Розквіт дешифрувального мистецтва Валліса припав на часи правління Вільгельма Оранського та його дружини Марії. Він продовжував служити криптоаналітиком і складав звіти для графа Нотінгемського, командувача морськими та сухопутними збройними силами Англії. Напруження, з яким він працював у ті роки, відбилося у одному з його листів:». боюся, що взагалі збожеволію».

У 1689 році Валлісу вдалося «розкрити» шифр листування короля Франції Людовика XIV і французького посла у Польщі, тим самим здійснити значний вплив на зовнішню політику Англії. Зокрема, він розкрив наміри Людовика XIV втягнути Польщу у війну проти Пруссії. В результаті ефективне використання цієї інформації дипломатією Англії призвело до того, що французькі посланці були з ганьбою вигнані з Польщі.

Після смерті Валліса Англія зробила важливий політичний крок: офіційно оголосила про введення урядової посади криптографа-дешифрувальника. У 1703 році першим офіційно оголошеним дешифрувальником Англії став внук Валліса – Уільям Бленкоу. Він працював достатньо успішно, але не витримав робочого напруження. У нападі тимчасового божевілля Бленкоу вчинив самогубство.

Не відставала й Франція, де дешифрувальне відділення було створено при Людовику XIII за пропозицією кардинала Рішельє. Його очолив Антуан Россиньоль (1600—1682), який створив дипломатичний шифр, що представляв собою складово-словниковий код на 600 компонентів.

Антуан Россиньоль уперше придбав популярність у 1626 році. Йому передали зашифрований лист, захоплений у кур'єра, що пробирався з обложеного міста Реальмон, і до кінця дня він дешифрував його. З листа стало зрозуміло, що армія гугенотів, що утримувала місто, перебуваючи на грані загибелі. Французи, які до цього не підозрювали про розпачливе положення гугенотів, повернули лист разом з його розшифровкою. Тепер гугеноти знали, що їхній супротивник не відступить, і негайно здалися. Так перемога французів стала результатом дешифрування.

Могутність криптології сталася очевидною, тому Антуан Россиньоль і його син Бонавентур одержали високі посади при дворі. Видатна майстерність і накопичений досвід з розкриття шифрів дозволив Россиньолям зрозуміти, як створити більш стійкий шифр, і вони придумали так званий «Великий шифр». Він застосовувався для зашифровування найбільш таємних повідомлень короля, приховуючи деталі його планів, задумів і політичних інтриг. В одному з цих повідомлень згадувалася одна з найбільш загадкових особистостей у французькій історії, людина в залізній масці, але стійкість «Великого шифру» означала, що повідомлення залишиться нерозшифрованим і непрочитаним протягом двох сторіч.

«Великий шифр» виявився настільки надійним, що зумів протистояти зусиллям всіх криптоаналітиків тієї епохи, що намагалися вивідати французькі таємниці, і навіть наступних поколінь дешифрувальників. На жаль, після смерті батька й сина «Великий шифр» пере-

став застосовуватися, а його подробиці були швидко загублені, що означало, що зашифровані папери у французьких архівах більше не можна було прочитати.

Цей шифр французька армія буде використовувати більше 100 років. Відомо, що навіть Наполеон під час своїх походів використовував шифри, що були спрощеними варіантами шифру Россиньолів. Не менш відомим був і «шифр Рішельє» – при його використанні текст повідомлення розбивався на відрізки, букви яких переставлялися у визначеному порядку. Россиньолю належить також авторство відомої доктрини про те, що «стійкість військового шифру повинна забезпечити таємність повідомлення протягом терміну, необхідного для виконання наказу. Стійкість дипломатичного шифру повинна забезпечувати таємність протягом декількох десятків років».

Россиньолі надзвичайно плідно працювали в сфері криптоаналізу як при дворі Людовика XIII, так і у свиті Людовика XIV. Наприклад, захоплення фортеці Еден королівською армією було прискорено завдяки тому, що Россиньолі прочитали зашифроване прохання її захисників про допомогу, а після цього тим же шифром склали відповідь, у якому жителі міста сповіщалися про даремність їхніх надій. Вони ніколи нікому не розповідали про те, скільки інших міст мусили скласти зброю і скільки зрад розкрили серед вищої знаті. Через цю їхню таємничість деякі придворні стверджували, що насправді Россиньолі не розкрили жодного шифру і кардинал поширював чутки про їхні здібності з метою попередження потенційних змовників.

На смертному одрі Людовик XIII охарактеризував Антуана Россиньоля як людину, від якого залежало благополуччя його підданих. Не дивно, що через два роки, 18 лютого 1645 року, спадкоємець Рішельє кардинал Мазаріні призначив Россиньоля державним радником. Як і Рішельє, Мазаріні пересилав йому перехоплені шифроповідомлення. Наприклад, у 1656 році він направив зашифрований лист кардинала Реца з указівкою Россиньолю прочитати його. При Людовику XIV Россиньоль часто працював у кімнаті, що безпосередньо прилягала до кабінету короля у Версальському палаці. Звідси йшов весь потік дешифрованих ним повідомлень, що допомагали королю визначати політику Франції.

Одним із кращих друзів Россиньоля був поет Буаробер, ініціатор ідеї створення Французької академії. Коли Буаробер потрапив у немилість при дворі, він поскаржився на нещастя, що звалилося на нього, у вірші, адресованому своєму впливовому другу-криптоаналітику. Россиньоль показав цей вірш Мазаріні, який під час наступної аудієнції привселюдно похвалив Буаробера. Пізніше з почуття подяки Буаробер написав 66-рядковий вірш, у якому оспівував Россиньоля. Це перша віршована ода, присвячена криптоаналітику. Деякі її рядки звучать так:

Яке дивовижне твоє мистецтво і яскраве.
І яка важлива сила твоєї майстерності!
Тому що з її допомогою здобуваються провінції,
Розкриваються секрети всіх королів,
І з малими зусиллями вона
Змушує здаватися міста й форти.
…Дійсно, твоя майстерність
Вище мого розуміння,
І я ніколи не осягну
Твій секрет; але я зараз можу сказати,
Що вона служить тобі дуже добре,
Що ти заслуговуєш її. Не побоюся,
Твоя майстерність буде благоволіти тобі роками.
І доля буде тобі посміхатися,
Поки війни затьмарюють землю.

Праця Россиньолів зробила його видною фігурою при дворі Людовика XIV. Саме йому вдалося довести правителям Франції надзвичайну важливість дешифрування депеш для фор-

мування їхньої політики. Його робота демонструвала це настільки ефективно, що королівський військовий міністр Лувуа став енергійно заохочувати кожного, хто міг надати отриману таким чином інформацію. Зберігся лист Лувуа, у якому той висловлював подяку за добутий шифр ворога, завіряючи, що людині, спроможній прочитати декілька шифрованих листів, «його величність подарує усе, що він попросить».

Россиньоль став першою людиною, що прославилася винятково завдяки своїм криптоаналітичним здібностям. Даниною загального захоплення вмінням «зламувати» шифри було те, що слово «россиньоль» стало французькою жаргонною назвою відмички. Шарль Перо, який більше відомий як автор казок, вніс біографію Россиньоля у свою книгу «Знамениті люди Франції в нинішнім столітті» поряд з життєписом Рішельє.

Після смерті Россиньоля у 1682 році «Великий шифр» вже не завжди застосовувався у королівському листуванні, і ця необачність дорого обійшлася Франції. Так, у 1774 році Людовику XV був доставлений пакет із Відня від секретаря французького посольства абата Жоржеля. Коли французький король розкрив його, то знайшов там копії відкритих текстів своєї шифрованої кореспонденції, що була «розкрита» у віденському ЧК.

У Німеччині був створений спеціальний орган – «криптографічна лабораторія» – під керуванням графа Гронсфельда, який удосконалив шифр Віженера, замінивши буквений ключ цифровим, цифри в якому позначали кількість кроків, на яке букву повідомлення зрушували вправо за алфавітом. Для цього під повідомленням писали ключ. Якщо ключ коротший повідомлення, то його повторювали циклічно. Шифровку одержували начебто за шифром Цезаря, але відраховували необов'язково тільки третю букву за алфавітом, а ту, яка була зрушена на відповідну цифру ключа. Завдяки простоті застосування цей шифр використовувався у той час надзвичайно широко.

Застосуємо як ключ групу з трьох початкових цифр числа «п» (314) та зашифруємо слово «ШИФРОВКА». Щоб зашифрувати першу букву повідомлення «Ш», використовуючи першу цифру ключа «3», відраховується третя одна за одною від «Ш» у алфавіті буква «Ш-Щ-Ю-Я» і виходить буква шифровки «Я». Далі використовуючи другу цифру ключа «1», відраховується перша від «И» у алфавіті буква ««И-І» і виходить буква шифровки «І» і так далі. В результаті отримуємо шифротекст:

відкритий текст …ШИФРОВКА
ключ……314314314
шифротекст ……ЯІШУПЕНБ

У той час також і Швеція приділяла увагу захисту власного дипломатичного та військового листування. Так, у 1676 році, за кілька днів до битви між шведською і датською арміями під містом Лунд, шведський король Карл XI відправив генералу Фабіану фон Ферсену шифрований лист зі своїми міркуваннями щодо стратегії й тактики військ у майбутній битві. Завдяки цій інформації шведи здобули перемогу в битві, яка стала однією з найкривавіших в історії Скандинавії.

У XVII столітті свій внесок у розвиток криптоаналізу зробив англієць Джон Фальконер. У 1685 році він написав книгу «Розкриття таємних повідомлень, або Мистецтво здобувати таємні відомості без ключа» (англ. *Cryptomensis Patefacta: or the art of secret information disclosed without a key),* де виклав деякі розроблені ним методи дешифрування. Зокрема, він запропонував використовувати перебір можливих відкритих слів за їх довжиною (якщо у шифротексті слова розділялися).

До кінця XVII століття криптологія остаточно склалася як наукова дисципліна. Хоча в даний період панували «номенклатори», які не були шифрами в «чистому» вигляді, проте поява багатоалфавітної заміни, використання трафаретів, біграм і цифрових позначень стала величезним кроком уперед у порівнянні з найдавнішим періодом і персоніфікувала наступ нової ери в розвитку криптології, що впритул наблизилася до свого сучасного вигляду.

Однак XVIII століття стало для криптології періодом «застою», або навіть «занепаду». Великий «стрибок», який ця наука зробила в попередній період, дозволив упродовж майже 150 років не вводити ніяких нововведень у способи шифрування й дешифрування повідомлень. Розроблені раніше криптосистеми успішно застосовувалися на практиці, а трактати XVI—XVII століть служили навчальними посібниками для крип-тоаналітиків. Майже всюди до криптологічної діяльності залучалися видатні вчені, в основному, математики, однак жоден з них в XVIII столітті не залишив будь-якої значимої праці з криптології, не розробив нової шифросистеми або придумав більш ефективного способу дешифрування.

Існуючі шифри заміни були досить стійкі, але й кваліфікація криптоаналітиків була високою настільки, що більшість значимих повідомлень розшифровувалася. Цей час став періодом розквіту «номенклатора» (лат. *nomen* – ім'я і *calator* – раб, слуга) – шифру, що представляв собою сполучення шифру заміни та невеликого коду. Він зазвичай містив кодові еквіваленти букв алфавіту та найбільш уживаних складів, слів і словосполучень, а також ряд спеціальних символів. Найчастіше в ньому траплялися спеціально створені для цієї мети символи, але нерідко також використовувалася астрологічна й окультна символіка.

Номенклатор був розроблений як система шифрування, що була найкраще пристосована до методів криптоаналізу, які найчастіше використовувались у той час. Вони, як правило, містили підрахунок частоти появи в тексті кожного символу та пошук у шифротексті слів і виразів, що містили характерні для даної мови сполучення букв. Метод частотного аналізу букв був заснований на тому, що в будь-якій мові одні букви зустрічалися частіше, ніж інші. В англійській мові, наприклад, частіше, ніж інші траплялася буква «*E*». Іншими буквами, що найбільш часто зустрічалися, були *T, A, O, N, R* і *S*. А букви *J, K, X* і *Z* траплялися в англійській мові рідко. Оскільки в ході операції заміни частота букви не змінювалася, ключ до розгадки значення того або іншого шифросимволу полягала іноді в підрахунку частоти його появи в шифротексті. Так само операція простої заміни не вносила змін і в сполучення букв (буквені моделі).

Цей тип криптосистеми, що поступово ускладнювався протягом трьох попередніх століть, досяг в XVIII столітті піка свого розвитку. Стандартним був розмір «номенклатора» в 400—500 символів, але були й такі, які досягали 5—6 тисяч та заміняли особливими символами практично всі значимі поняття, імена, назви й цілі речення. У цей період «номенклатори» стали схожі більше не на шифр, а на форму ієрогліфічного листа, і незважаючи на це, їх все-таки «розкривали».

Конец ознакомительного фрагмента.