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

Вадим Гребенников

Американська криптологія. Історія спецзв'язку

http://www.litres.ru/pages/biblio_book/?art=36076207
ISBN 978-5-4493-0774-3

Аннотация

Книга розповідає про історію народження й розвитку криптології у США, розробки та застосування шифрувальних машин, а також утворення американських криптологічних служб, «шпіонську» діяльність спецслужб США та їхню боротьбу у «полюванні» за радянськими шифрами.

Книга побудована виключно на відкритих матеріалах, зібраних автором із надрукованих книг та мережі Інтернет.

Офіційна веб-сторінка книги: http://cryptohistory.ru

Содержание

Американська криптологія
Історія спецзв'язку

Вадим Гребенніков

ISBN 978-5-4493-0774-3
Создано в интеллектуальной издательской системе Ridero

1. Стан криптології до XX ст.

За океаном, у Північній Америці, у XVIII столітті не було ні «чорних кабінетів», ні будь-яких криптослужб. Разом з тим, відомо, що американські делегати у Франції та державний секретар під час скандальної справи «Ікс-Ігрек-Зет» (англ. *X-Y-Z)* у 1737 році, повязаної з вимаганням французькими посадовими особами грошових «подарунків» від американців, шифрували своє листування за допомогою номенклатора.

Наприкінці XVIII століття розпочалася війна за незалежність США (1775-1783) між королівством Великобританії і лоялістами (прибічниками британської корони) з одного боку та революціонерами 13 англійських колоній (патріотами) з іншого, які проголосили свою незалежність від Великобританії, як самостійна союзна держава. 29 листопада 1775 року патріоти утворили такий державний орган як Комітет для секретної кореспонденції з друзями колоній у Великобританії, Ірландії та інших частинах світу. Наприкінці 1977 року він був реорганізований у Комітет закордонних справ (з 1789 року – Держдепартамент) США.

Повстанці як могли боролися з англійськими шпигунами, однак перехоплювати криптограми англійців їм вдавалося дуже мало. І лише коли війна наближалася до свого завершення та була захоплена достатня кількість шифрова-

них повідомлень, були організовані «разові групи» з дешифрування. В одну з таких груп входив майбутній віце-президент США Елбрідж Джеррі. Головним напрямком роботи цих груп було виявлення англійських шпигунів і дешифрування листування англійських військ. Більшість з криптограм було дешифровано Джеймсом Ловелєм (1737—1814), якого можна по праву назвати «батьком» американського криптоаналізу.

У 1777 році Ловель був обраний депутатом Конгресу, членом Комітету закордонних справ і незабаром став відомий завдяки своїй запопадливості та працьовитості. Одним з перших обов'язків Ловеля була розшифровка листів Чарльза Дюма, американського дипломата, що жив в Нідерландах і пізніше представляв інтереси США в Європі. Саме Дюма винайшов перший дипломатичний шифр Континентального Конгресу, який використовувався американським дипломатом у Франції Бенджамином Франкліном для листування з агентами а Європі.

Восени 1781 року американський командувач на півдні Натаніель Грін направив Конгресу кілька перехоплених англійських криптограм, які у його штабі ніхто не міг прочитати, додавши їх до свого загального повідомлення. Ця шифрована англійська кореспонденція виявилася листуванням між заступником головнокомандувача англійських військ в Америці Корнуолісом і його підлеглими.

Повідомлення Гріна було зачитано в Конгресі 17 вересня.

Чотирма днями пізніше Ловель розшифрував додатки до повідомлення. На жаль, через швидкий розвиток подій добута ним інформація не принесла багато користі. Але знайдені Ловелєм ключі цілком могли згодитися коли-небудь у майбутньому. У своєму листі Вашингтону він написав: «Не виключено, що супротивник має намір і далі зашифровувати своє листування… Якщо це так, то ваше превосходительство, можливо, побажає отримати для себе користь, давши вашому секретарю вказівку зняти копію ключів і зауважень, що я через вас направляю…»

Більш проникливим Ловель бути не міг. Розкритий ним шифр дійсно служив також і для зв'язку між Чарльзом Корнуолісом і генералом Генрі Клінтоном, що знаходився в Нью-Йорку. На той час Корнуоліс відступив до Йорк-Тауна, щоб дочекатися підкріплень від Клінтона. До речі, Клінтон зашифровував свої повідомлення, використовуючи номенклатор, алфавітну таблицю, ряд замін і решітку.

Але Вашингтон з 16-тисячним військом оточив місто, а французький адмірал граф де Грасс із 24 кораблями заблокував допомогу англійцям з моря. 6 жовтня Вашингтон писав Ловелю: «Мій секретар зняв копії з шифрів і за допомогою одного з алфавітів зумів розшифрувати параграф недавно перехопленого листа лорда Корну-оліса серу Клінтону». Ця інформація допомогла Вашингтону оцінити реальний стан справ в англійському таборі.

Тим часом для зв'язку з Корнуолісом Клінтон спорядив

два невеликі судна, які він відправив з Нью-Йорка 26 вересня і 3 жовтня. Однак вони були захоплені повстанцями. При цьому одне з них прибило до берега, де англієць, який віз пачку шифрованих депеш, сховав їх під великим каменем, перш ніж його захопили в полон. Потім, як висловився один з очевидців, «у результаті нетривалої бесіди, пообіцявши прощення», повстанці умовили англійця віддати заховані депеші.

Ловель одержав ці депеші 14 жовтня та відразу приступив до справи. Успіх не змусив себе довго чекати, тому що він з'ясував, що вони були зашифровані тим же шифром, що й інше листування Корнуоліса. Через п'ять днів після того, як Ловель закінчив дешифрування, Корнуоліс капітулював.

Але перемога повстанців була не зовсім повною. Вашингтон зрозумів це, коли наступного дня він нарешті одержав від Ловеля копії дешифрованих депеш. Не втрачаючи ні хвилини, Вашингтон переправив їх де Грассу, кораблі якого повинні були перешкодити спробі надання допомоги Корнуолісу Грейвсом і Клінтоном. Будучи попередженим, французький адмірал ґрунтовно підготувався до нападу англійців. 30 жовтня він змусив англійський флот відступити й тим самим наблизив остаточну перемогу американців у війні за незалежність.

Пізніше Ловель винайшов власний поліалфавітний шифр. Цей шифр активно використовувався Ловелєм в його листуванні. Проте, як з'ясувалося пізніше, шифр став відомий

тим, що постійно заплутував кореспондентів Ловеля. У його шифрі кореспонденти формували таблицю замін з узгодженого ключового слова. Спочатку в стовпець записувалися числа від 1 до 27, потім поряд з ним записувався стовпець з 27 букв алфавіту (a-z і &), починаючи з першої букви ключового слова. Потім аналогічний стовпець, що починався з другої букви ключового слова, і так далі. При шифруванні стовпці використовувалися по черзі, і кожна буква шифрувалася числом. Як видно, якщо при шифруванні допущена помилка, тобто наприклад один стовпець використовувався двічі підряд, процес розшифрування відразу ж заплутувався.

У цілому, ефективність дешифрування повстанців виявлялася досить високою завдяки тому, що англійські шифри й ключі не мінялися тривалий час. Крім того, мережа шифрованого зв'язку Англії в США мала істотний недолік: усі командири військових підрозділів використовували для зв'язку між собою та Лондоном ті ж самі шифри й ключі. У цих умовах дешифрування повідомлень одного з абонентів приводило до компрометації листування всіх абонентів мережі. В результаті американцям вдавалося одержувати інформацію, досить важливу для проведення своїх військових операцій.

Посланець США у Франції, член Комітету закордонних справ, учений, дипломат, філософ Бенджамін Франклін (1706—1790) для зв'язку з Конгресом розробив свій

власний шифр багатозначної заміни. Цікавий був сам спосіб складання шифру. Він узяв відрізок французького тексту (682 букви), пронумерував у ньому знаки і кожній букві латинського алфавіту додав безліч позначень (чисел) у пронумерованому тексті. При шифруванні кожна буква замінялася на довільно обране число з безлічі позначень.

У сучасному розумінні він використовував шифр пропорційної заміни, у якому кількість можливих шифропозначень пропорційна частоті повторюваності букв у відкритому тексті. При використанні такого шифру знаки шифрованого тексту з'являлися приблизно з однаковими частотами. Розробивши власний шифр пропорційної заміни, Франклін відтворив ідею шифру, запропонованого Габріелем де Лавінда ще в XV столітті.

На жаль (для американців), один із помічників Франкліна – генеральний секретар американської місії у Франції Едуард Банкрофт – був англійським шпигуном. В результаті Франклін часто відправляв в Америку дезінформацію, надану йому Банкрофтом. Інший помічник Франкліна, Артур Лі, користувався своєрідним книжковим шифром. Відкритий текст шифрувався не по буквах, а словах. Ключем шифру був заздалегідь обговорений словник, а всі слова мінялися на відповідні номери сторінок і слів на сторінці. Однак цей шифр виявився досить незручним у застосуванні.

У 1779 році конгресмен і офіцер континентальної армії Бенджамін Толмадж (1754 -1835) розробив для зв'язку з Ва-

шингтоном номенклатор, який складався з одного розділу та 760 елементів. Для цього він використав найбільш уживані слова з «Нового орфографічного словника» Джона Ентіка. Виписавши у стовпець обрані слова, Толмадж привласнив кожному з них визначене число, а географічні назви та імена людей помістив у окремий розділ. Слова у номенклаторі були розташовані у буквено-цифровій послідовності, а крім того, номенклатор містив також перемішаний алфавіт для кодування слів і чисел, що не увійшли у список.

У 1781 році Секретар закордонних справ США Роберт Лівінгстон (1746—1813) розробив номенклатор, який містив упорядковану за алфавітом групу слів і складів на одному боці та числа від 1 до 1700 на іншому. Скориставшись системою Лівінгстона, майбутні держсекретарі та президенти США Томас Джеферсон (1743—1826) і Джеймс Медісон (1751—1836) розробили свою власну систему захисту листування. Вона виявилася зручнішою, оскільки дозволяла вставляти букви або числа у відкритий текст при будь-яких обраних відправником і адресатом кодових комбінаціях.

Крім того, Медісон як член вірджінської делегації на Континентальному конгресі користувався номенклатором, який складався приблизно з 846 елементів, щоб надсилати приватні листи губернатору штату Віргінія Бенджаміну Гарісону. Його система складалася щз перечня чисел, букв, складів і географічних назв, таких як Відень тощо. З 1801 року Медісон, перебуваючи на посаді державного секретаря США,

для листування з Лівінгстоном, який у той час був послом у Франції, користувався номенклатором, що мав 1700 елементів. З 1803 року Медісон листувався зі своїми представниками Лівінгстоном і Джеймсом Монро вже новим кодом, який отримав назву «шифр Монро». Хоча ця система була названа шифром, вона мала усі властивості номенклатора, 1600 елементів якого були розташовані у алфавітному порядку.

У 1790-х роках американська криптологія збагатилася чудовим винаходом. Його автором був державний діяч, перший державний секретар, а потім і президент США Томас Джеферсон. Свою систему шифрування він назвав «дисковим шифром». Цей шифр реалізовувався за допомогою спеціального пристрою, що згодом назвали «шифратором Джеферсона». Конструкція шифратора може бути коротенько описана таким чином.

Дерев'яний циліндр розрізався на 36 дисків (у принципі, загальна кількість дисків може бути й іншою). Ці диски насаджувалися на одну загальну вісь таким чином, щоб вони могли незалежно обертатися на ній. На окружності кожного з дисків виписувалися всі букви англійського алфавіту в довільному порядку. Послідовність букв на різних дисках була різною. На поверхні циліндра виділялася лінія, рівнобіжна його вісі. При шифруванні відкритий текст розбивався на групи по 36 знаків, потім перша буква групи фіксувалася положенням першого диска по виділеній лінії, друга – поло-

женням другого диска й так далі. Шифрований текст утворювався шляхом зчитування послідовності букв по будь-якій рівнобіжно виділеній лінії.

Зворотний процес здійснювався на аналогічному шифраторі: отриманий шифротекст виписувався шляхом повороту дисків по виділеній лінії, а відкритий текст відшукувався серед рівнобіжних їй ліній шляхом прочитання осмисленого можливого варіанта. Хоча теоретично цей метод дозволяв припустити появу різних варіантів відкритого повідомлення, але, як показав накопичений того часу досвід, це було малоймовірно: осмислений текст читався тільки по одній з можливих ліній. Шифратор Джефферсона реалізовував раніше відомий шифр багатоалфавітної заміни. Частинами його ключа був порядок розташування букв на кожному диску та порядок розташування цих дисків на загальній осі. Загальна кількість ключів була величезна.

Цей винахід став провісником появи так званих дискових шифраторів, що знайшли широке поширення в розвинутих країнах у XX столітті. Шифратор «М-94», який був аналогічний шифратору Джефферсона, використовувався в армії США під час Другої світової війни. Однак при житті Джефферсона доля його винаходу склалася невдало. Будучи держсекретарем, сам Джефферсон продовжував використовувати традиційні коди (номенклатори) та шифри Віженера. Він дуже обережно відносився до свого винаходу та вважав, що його потрібно ґрунтовно проаналізувати. З цією метою він

тривалий час підтримував зв'язок з математиком Р. Патерсоном.

В результаті обміну інформацією Патерсон запропонував свій власний шифр, який, на його думку, був більш надійним, ніж шифр Джеферсона. Він являв собою шифр вертикальної перестановки з уведенням «пустишок». За своєю стійкістю він значно поступався шифру Джеферсона, однак той прийняв доводи свого опонента та визнав його шифр більш прийнятним для використання. Таким чином, Джеферсон сам не оцінив усієї значимості свого власного винаходу.

У 1817 році полковник американської армії, начальник артилерійсько-технічної служби армії США Д. Уодсворт також запропонував свій механічний шифратор. Основними елементами пристрою були два шифрувальні диски. По окружності першого з них (верхнього), що реалізовував алфавіт відкритого тексту, за абеткою були розташовані 26 букв англійського алфавіту. На другому (нижньому) диску з алфавітом шифрованого тексту в довільному порядку розташовувалися ці ж букви та цифри від 2 до 8. Таким чином, він містив 33 знаки. Літери на диску були зйомними, що дозволяло змінювати алфавіт шифрованого тексту. Диски були з'єднані між собою шестерною передачею з числом зубів 26 х 33.

При обертанні першого диска (за допомогою кнопки) на один крок другий диск обертався також на один крок в ін-

ший бік. Оскільки числа 26 і 33 були взаємно простими, то при покроковому обертанні першого диска обидва диски поверталися у початковий стан через 26 х 33 = 858 кроків. Диск відкритого тексту обертався тільки в один бік. Диски містилися у футлярі, у якому були прорізані вікна. За допомогою спеціальної кнопки шестірні роз'єднувалися, що дозволяло незалежно один від одного повертати диски в початкове для шифрування положення (за допомогою додаткових кнопок). Довгостроковим ключем був алфавіт шифрованого тексту (їхня кількість була 33), а разовий ключ складався з двох букв (верхнього та нижнього диска) і встановлювався у вікнах при незалежному повороті дисків. Кількість разових ключів була: 26 х 33 = 858.

Шифрування вироблялося таким чином. Перед початком шифрування диски ставилися в початкові умовні положення (наприклад, *LB*). Потім шестірні з'єднувалися, і за допомогою кнопки диск повертався доти, поки у верхньому вікні не з'являлася перша буква відкритого тексту. З вікна під ним списувалася перша буква шифрованого тексту. Інші букви шифрувалися аналогічним чином. Якщо букви повторювалися (наприклад, *AA*), то диск робив повний оберт, тому в шифротексті цій парі відповідали пари з різних знаків (наприклад, *8B).*

Розшифрування робилося зворотним чином. Букви шифрованого тексту встановлювалися по нижньому вікну, а з верхнього списувалася відповідна буква відкритого тексту.

Даний шифр мав такі особливості:

– кількість знаків в алфавіті шифрованого тексту (33) була більше кількості букв в алфавіті відкритого тексту (26);

– шифрування букви відкритого тексту залежало від того, якою була попередня їй буква, що шифрувалася.

Пропозиція Уодсворта заслуговувала на увагу, незважаючи на те, що недоліком шифру була його особлива чутливість до неточностей (типу заміни та пропуску знаків у шифрованому тексті). Перекручена або пропущена буква робила весь наступний текст при розшифруванні незрозумілим. Однак історична відмова від запропонованої системи шифрування була пов'язана з іншими обставинами. В ці роки панували так звані «ручні шифри», застосування яких не вимагало спеціальних пристосувань. Ці шифри були добре засвоєні, їм вірили та їх добре знали, у зв'язку з чим пропозиція Уодсворта породжувала зайві «турботи».

Всередині XIX століття американець П. Е. Чейз запропонував модифікацію відомого шифру Полібія (див. таблицю).

	1	2	3	4	5	6	7	8	9	0
1	X	U	A	C	O	N	Z	L	P	φ
2	B	Y	F	M	@	E	G	J	Q	ω
3	D	K	S	V	H	R	W	T	I	λ

Ключем шифру був порядок розташування букв у таблиці. При шифруванні координати букв виписувались вертикально. Наприклад, слово «UKRAINE» можна записати як такий дворядковий цифровий шифротекст:

1 3 3 1 3 1 2

2 2 6 3 9 6 6

Чейз запропонував ввести ще один ключ: заздалегідь обговорене правило перебудови нижнього рядка цифр. Наприклад, число, визначене цим рядком, помножувалося на 9: 2263966 x 9 = 20375694, після чого отримувався новий шифротекст:

1 3 3 1 3 1 2

2 0 3 7 5 6 9 4

Цей дворядковий запис знову перетворювався у букви згідно з вищезазначеною таблицею, при цьому перше число (2) визначало букву першого рядка. В результаті отримуємо такий шифротекст: UφSWORPM.

Шифр Чейза був більш стійким за шифр Полібія, однак розповсюдження він не мав. Його недоліками були значне ускладнення процесу шифрування-розшифрування та особлива чутливість шифру до помилок (перекручування у шифротексті).

В другій половині XIX століття відбулася революція у військовій справі. З'явилися нові засоби збройної боротьби (парові кораблі, нарізні артилерія та стрілецька зброя), комунікацій (залізниця) та зв'язку (телеграф). Поява телегра-

фу змістовно вплинула на розвиток криптології.

Однією з війн, у якій широко застосовувалися перераховані новинки, стала громадянська війна в США (1861—1865) між мешканцями Півночі (далі – федерали) та Півдня (далі – конфедерати). Перемогу в цій війні одержали федерали, що в результаті привело до створення США в їхньому сучасному вигляді. У цій перемозі помітну роль зіграла перевага федералів у криптологічних методах. При цьому федерали часом «винаходили» заново шифри, що були добре відомі в Європі.

У той час для передачі повідомлень вже широко використовувався телеграф. Щоб телеграфіст міг легко читати переданий текст, шифротексти повинні були бути максимально наближеними до звичайних відкритих текстів. При передачі шифротекстів, що представляли собою хаотичний набір букв, телеграфісти робили численні помилки, що істотно ускладнювало наступне розшифрування. Крім того, помилки виникали через збої при роботі телеграфних апаратів. Наприклад, для американського апарата «Морзе» були характерні помилки при передачі, за результатом яких у тексті одна буква виявлялася зайвою, або навпаки, однієї букви не вистачало. У випадку «хаотичних» шифротекстів такі перекручування нерідко приводили до неможливості розшифрування.

Крім телеграфу застосовувалися й інші способи передачі інформації, зокрема, «прапорцеві» коди. У 1856 році офіцер

медичної служби Альберт Джеймс Майер (1828—1880) запропонував метод зв'язку з використанням сигнальних прапорців – прапорцевий семафор (англ. *wig-wag).* Для представлення різних букв використовувалися різні положення прапорця, і в такий спосіб солдати передавали повідомлення. «Прапорцеву» систему Майера застосовували як солдати північної коаліції, так і конфедерати. Для цього використовувалися природні височини. Якщо таких не виявлялося, то будувалися спеціальні вишки.

Тепер розглянемо шифри, якими користувалися федерали та конфедерати під час Громадянської війни в США. Найбільше поширення у федералів мав шифр, що включав елементи кодування та перестановки слів. Найбільш таємні слова тексту попередньо замінювалися за допомогою довгострокового коду. Наприклад, слово *«COLONEL»* замінювалося на *«VENUS».* Аналогічно, фраза *«PRESIDENT OF USA»* замінювалася на слово *«ADAM»* тощо. Заміна на позначення, що легко читалися, полегшувала роботу телеграфістів, які передавали шифровані повідомлення.

Потім кодований текст виписувався за словами порядково в прямокутник, що містив визначену кількість стовпців. Кількість стовпців у відкритому вигляді передавалося в шифрованому тексті у вигляді якого-небудь слова. Наприклад, слово *«GUARD»,* яке стояло на початку телеграми, означало, що в прямокутнику 5 стовпців (кількість букв у слові). Потім з отриманого прямокутника слова випису-

валися, наприклад, за таким правилом: перший стовпець – зверху донизу, другий – знизу нагору, третій – зверху донизу тощо. Виходив остаточний шифрований текст, що й передавався телеграфом.

Цей шифр був запропонований у 1861 році Ансоном Стейджером, першим керівником компанії «Вестерн Юніон телеграф». Після мобілізації він був призначений керівником управління військового телеграфу в Огайо. Ще до війни Стейджер запропонував такий шифр для губернатора штату Огайо, що з успіхом використовувався останнім у листуванні зі своїми колегами – губернаторами штатів Індіана й Іллінойс.

У 1862 році завдяки першому масштабному використанню телеграфа у військових цілях шифр Стейджера почав застосовуватися всією армією Півночі. Досвід роботи Стейджера на телеграфі, вочевидь, привів його до системи, у якій шифротекст складався, як і в нових телеграфних кодах, зі звичайних слів, що значно менше піддавалися перекручуванням, ніж групи довільно набраних букв. У ході війни до системи були введені деякі елементарні ускладнення, що її помітно підсилили. До написаного тексту вставлялися «пустишки». Виписка стала робитися по діагоналях і змінних стовпчиках у прямокутниках, що усе більше і більше збільшувалися.

С. Беквіт, шифрувальник командувача військами федералів Уіліса Гранта, запропонував, щоб важливі терміни пе-

редавалися кодовими позначеннями, які він ретельно вибирав, щоб звести до мінімуму телеграфну помилку. Цікаво відзначити, що крім військових цим шифром користувався й керівник розвідки Алан Пінкертон, майбутній засновник знаменитого детективного агентства.

Також використовувалися прості словникові перестановки. У цьому шифрі слова відкритого тексту переставлялися за визначеним законом (ключем). Цей шифр був досить слабким. Використовувався ще один вид шифрів – багатоалфавітні системи (стосовно алфавіту шифрованого тексту), у якому будувалася таблиця розміром 26х26 (число букв латинського алфавіту).

Стовпці таблиці позначалися буквами латинського алфавіту в порядку їхнього звичайного проходження *(A, B, C,*Z). Рядки таблиці були довільними перестановками цих букв. Це був алфавіт відкритого тексту, що визначав верхній рядок підстановки, за яким набиралися букви відкритого тексту. Рядки таблиці використовувалися в природному порядку (перший, другий тощо) і визначали нижній рядок підстановки. Перша буква тексту шифрувалася по першому рядку, друга – по другому тощо. Правило повторювалося циклічно (27-а буква тексту шифрувалася знову по першому рядку, 28-а – по другому тощо).

У липні 1865 року сержант Е. Хоулі запропонував використовувати для цього шифру віяло, що складалося з 26 дерев'яних дощечок, на яких були записані алфавіти шиф-

рованого тексту (рядки таблиці). Це віяло виявилося настільки ефективним у практичному застосуванні, що вперше в історії США його автору був виданий патент на шифропристрій.

У той час як федерали прийняли централізовану організацію системи зв'язку, конфедерати поширили принцип прав штатів і на сферу шифрувальної справи. Кожен командир міг за своїм розсудом вибирати власні коди та шифри. Це привело до істотних негативних наслідків, оскільки місцеві командири практично не розбиралися в шифрувальній справі.

Конфедерати використовували примітивні шифри аж до шифрів простої заміни. Наприклад, перед битвою в Шайлоу 6 квітня 1862 року генерал Джонстон домовився зі своїм заступником генералом Борегаром використовувати як військовий шифр заміну Цезаря. Зрідка вживалися книжкові шифри. Книжковим шифром користувався президент конфедерації південних штатів Джеферсон Девіс. Перед битвою під Шайлоу він послав генералу Джонстону словник для його використання як кодової книги. Додатком до словника була інструкція, в якій вказувалося, що слово «з'єднання» буде виражатися як «146.Л.20», що означало, відповідно, номер сторінки, лівий стовпчик і номер слова.

Словники використовувалися як кодові книги також у ВМФ конфедерації. Його міністр Стефан Мелорі особисто розпорядився, щоб командири кораблів здобули ідентичні примірники різних словників.

Поширені у той час були шифри типу Віженера. Збереглися, навіть, зразки таких шифрувальних пристроїв у вигляді мідних шифрувальних циліндрів. Шифрування здійснювалося за допомогою двох покажчиків (на верхній планці пристрою) на букви відкритого тексту та відповідні їм букви шифрованого тексту.

Як уже було сказано раніше, при шифруванні допускалися численні помилки. Помилками конфедератів успішно користувалися федерали для дешифрування перехоплених повідомлень. Зокрема, при використанні книжкових шифрів у якості вихідних шифровеличин вибиралися не букви, а слова й цілі вирази. При цьому конфедерати часто використовували загальнодоступні комерційні кодові книги, згідно з якими і робили заміну шифровеличин. Федералам не складно було перебирати обмежене число комерційних кодових книг і знаходити ключ. Для посилення кодування конфедерати вводили прості правила типу: якщо слово, що шифрувалося, знаходилося на 18-у місці 29-ї сторінки книги, то воно замінялося 18-м словом на 19-й сторінці. Однак подібні модифікації не бентежили федералів.

Шифрований зв'язок федералів здійснювався через Управління військового телеграфу, при якому була шифрувальна служба. Начальником військового телеграфу був майор Томас Екерт, який пізніше став головою правління компанії «Вестерн Юні-он телеграф». Управління військового телеграфу розміщалося в будинку військового міністер-

ства, що знаходилося поруч з Білим Домом. Президент Авраам Лінкольн приділяв велику увагу організації шифрованого зв'язку та часто спілкувався з трьома молодими телеграфістами-шифрувальниками: Девідом Бейтсом, Чарльзом Тінкером і Альбертом Чендлером. Ці люди були основними криптоаналітиками Півночі.

Криптоаналітична служба федералів досягла досить серйозних успіхів. Так, наприклад, у грудні 1863 року начальник поштового відділення Нью-Йорка Абрам Уейкман, переглядаючи кореспонденцію перед відправленням, наткнувся на лист, адресований Олександру Кейту до міста Галіфакс у Новій Шотландії. Про Кейта було відомо, що той часто листувався з агентами Півдня. Тому, розкривши конверт та встановивши, що лист зашифрований, Уейкман передав його військовому міністру.

Протягом двох днів співробітники Військового міністерства марно намагалися розгадати таємничі знаки перехопленої криптограми. Потім вона була передана шифрувальникам президента Лінкольна, що взялися її прочитати. Вони швидко встановили, що невідомий автор листа використовував для його зашифрування як звичайний алфавіт, так і 5 різних шифроалфавітів. Але він вчинив нерозсудливо, розділивши слова листа комами та обмеживши одним алфавітом у межах кожного слова.

Дешифрувальники знайшли слово, що складалося з шести букв, у якому друга й шоста букви повторювалися. По-

тім випливало слово з чотирьох букв, за яким у свою чергу йшла фраза, послана клером: «reaches you». Вони вирішили, що за цією послідовністю шифрознаків повинна ховатися фраза «before this». Бейтс припустив, що в листі використано шифр, подібний тому, що застосовувався для позначення цін у магазині в Пітсбурзі, де він колись давно працював посильним.

Цей здогад дозволив значно просунути вперед процес дешифрування криптограми. Допомогло й виявлення знаків, що позначали місце відправлення і дату – «Нью-Йорк, 18 грудня 1863 р.». Діючи таким чином, три шифрувальники у присутності президента Лінкольна, що нетерпляче очікував результати, за чотири години прочитали шифрований лист, у якому було написано:

«Нью-Йорк, 18 грудня 1863 р. …Два пароплави відбудуть звідси приблизно на Різдво… 12 тисяч нарізних мушкетів прийшли точно за адресою та відправлені в Галіфакс відповідно до інструкцій. Ми зможемо захопити ще два пароплави, як намічено… перш ніж це дійде до вас. Ціна 2000 доларів. Нам потрібно більше грошей… Пишіть як колись…»

Два дні по тому була перехоплена та швидко дешифрована ще одна криптограма, адресована Кейту. У ній говорилося: «Передай Меміджеру, що в Хілтона усі верстати знаходяться в зібраному вигляді та всі матриці будуть готові до відправлення 1 січня. Гравірування друкованих форм чудове».

Таким чином, з листа стало відомо, що форми для друкування грошей конфедератів виготовлялися в Нью-Йорку. Гравера Хілтона легко знайшли в Манхеттені. 31 грудня 1863 року поліцейські відвідали його помешкання, де захопили друковані верстати й матриці, а також уже видрукувані гроші на суму в кілька мільйонів доларів. Тим самим конфедерація позбавилася устаткування для виготовлення паперових грошей, яких їй бракувало. Головну роль у всій цій справі зіграли криптоаналітичні здібності, виявлені трьома молодими шифрувальниками Лінкольна. За це кожний з них одержав збільшення до зарплатні розміром у 25 доларів на місяць.

Усього за час війни Північ передала приблизно 6,5 мільйона телеграм. Конфедерати здійснювали перехоплення їхніх телеграфних повідомлень, багато з яких, зазвичай, шифрувалися. їхня кавалерія робила нальоти на пункти зв'язку, що приводило до компрометації систем шифрування федералів та дозволяло конфедератам одержувати ключі й інформацію про відкриті тексти, що відповідали відомим шифрованим текстам. Крім того, шифри федералів мали слабкості. Незважаючи на все це, конфедерати так і не навчилися розкривати шифровані повідомлення федералів.

Вони іноді, навіть, не могли правильно розшифрувати свої власні повідомлення, не дивно, що їм не вдалося прочитати жодного шифрованого повідомлення федералів. Цьому факту було б важко повірити, якби конфедерати самі

не визнали його, надрукувавши у своїх газетах кілька шифрованих повідомлень із проханням їхнього дешифрування.

Федерали також захоплювали шифри Півдня та здійснювали перехоплення кур'єрів із шифрованими повідомленнями. Так, наприклад, у 1863 році під час облоги міста Віксберга війська У. Гранта захопили вісім повстанців і в одного з них знайшли криптограму. її відправили до Вашингтона криптоаналітикам Президента, які успішно справилися з черговим завданням. Хоча дешифрування цієї телеграми не допомогло Гранту «взяти» Віксберг, але воно дало федералам один з ключів, якими конфедерати користувалися під час війни.

Шпіони як федералів, так і конфедератів зашифровували свої повідомлення дуже простими шифрами. Так, прихильниця Півночі Елізабет Ван Лью захищала свої агентурні донесення за допомогою буквено-цифрового шифру, основаного на квадраті Полібія. А прихильниця Півдня Роза Грінхоу захищала свої агентурні донесення за допомогою шифру випадкової заміни.

Із закінченням громадянської війни та перемогою федералів розробкою кодів і шифрів став займатися Державний департамент США. У 1867 році держсекретар Уільям Генрі Сьюард (1801—1872) розробив код Держдепартаменту на 148 сторінках. Однак процес кодування та декодування виявився для дипломатів дуже складним. Тому у 1871 році начальник корпусу зв'язку полковник Альберт Майер розро-

бив для Держдепартаменту код на 88 сторінках, що складався з однієї частини. Книга містила коди для часу діб, днів, місяців і – вперше в історії кодів – років. Вона стала першим кодом Держдепартаменту, в якому одному кодовому слову відповідала довга фраза або ціле речення. Для позначення часу доби як кодові сдова використовувались жіночі імена, а днів місяця – чоловічі. Назви міст і країн замінялися цифрами.

Наступну книгу державних кодів розробив у 1876 році завідувач бюро каталогів і архівів Держдепартаменту Джон Генрі Хасвел (1841—1899), який до цієї справи підійшов дуже змістовно та прискипливо. Багато років він займався питаннями стійкості кодів і дорожнечі телеграм, вивчав методи шифрування Майера і Стейджера часів Громадянської війни та комерційні коди, зокрема: телеграфний код Слейтера 1870 року. В результаті книга Хасвела, яка мала назву «Шифр Держдепартамента (1876)», містила найкращі риси кодів того часу та мала одну частину на 1200 сторінках. Оскільки вона мала червону обкладинку, пізніше код був названий «червоним» (англ. *red).* Для підвищення стійкості свого коду Хасвел розробив також «Доповнення до шифру Держдепартаменту: код, що не піддається декодуванню». У цьому доповненні перераховувались 50 правил, або способів перешифрування, які могли застосовуватися до закодованих повідомлень.

У 1878 році вперше в історії США вирішальну роль в аме-

риканській політиці був вимушений зіграти криптоаналіз. Все почалося з сенсаційної статті, надрукованої 7 жовтня газетою «Трибуна Нью-Йорка» (англ. *The New York Tribune).* У замітці, розміщеній під заголовком «Перехоплені шифровані телеграми», приводився відкритий текст декількох криптограм.

Справа в тому, що в результаті підрахунку голосів, поданих на виборах президента в 1876 році, першим виявився кандидат від Демократичної партії Самуель Тілден, що одержав на чверть мільйона голосів більше, ніж його суперник від Республіканської партії Рутерфорд Хейс. Але як розподіляться вирішальні голоси виборців – це залежало від того, які із суперечливих результатів голосування, проведеного двічі у Флориді, Луїзіані, Південній Каролині й Орегоні, будуть визнані дійсними. Конгрес створив спеціальну комісію для вирішення цього питання, яка постановила віддати всі спірні голоси виборців Хейсу. Це забезпечило йому більшість усього в один голос у колегії виборців і посаду Президента США.

На сесії Конгресу, що відбулася після виборів Президента, була призначена ще одна спеціальна комісія для розслідування поширених демократами слухів про «купівлю» республіканцями голосів вибірників. У ході розслідування комісія конфіскувала більше 600 шифротелеграм, що були послані різними політичними діячами та їх довіреними особами під час виборчої кампанії в чотирьох штатах. Інші аме-

риканська телеграфна компанія «Вестерн Юніон» на той час уже встигла знищити, щоб показати, що гарантує таємницю довіреного їй листування.

У 1875 році 27 шифротелеграм були таємно передані до прореспубліканської газети «*The New York Tribune*» у надії на те, що будучи дешифровані, вони поставлять демократів у скрутне становище. Цікаво, що редактор газети Уайтлоу Рейд вирішив не обмежуватися публікацією шифротелеграм своїх політичних супротивників. Він особисто взявся за «розкриття» шифролистування демократів із метою оприлюднення їхніх відкритих текстів.

Багато читачів, спонукувані редакційними статтями газети, пропонували свої варіанти дешифрування опублікованих шифротелеграм, але при перевірці усі вони виявилися невірними. Тим часом газета «Детройт пост» зуміла вивідати в одного з демократів, яким саме шифром користувалися його партійні соратники під час передвиборчої кампанії в Орегоні. Шифрувальник відшукував потрібне слово в «Домашньому англійському словнику», що був виданий у Лондоні в 1876 році, визначав порядковий номер цього слова на сторінці, відраховував 4 сторінки назад і брав на ній відповідне слово як кодове позначення. Для розшифрування отриманого повідомлення його адресат робив навпаки.

4 вересня 1878 року один з редакторів *«The New York Tribune»* Джон Хассард, ґрунтуючись на інформації газети «Детройт пост», опублікував кілька відкритих текстів

дешифрованих криптограм, з яких випливало, що в Орегоні демократи прагнули підкупити одного республіканського виборця, однак угода не відбулася тільки через затримку з передачею йому грошей.

Але «Домашній англійський словник» мало допомагав у дешифруванні повідомлень демократів, надісланих з інших трьох штатів. Не розраховуючи більше на сторонню допомогу, Рейд запропонував своїм співробітникам зайнятися їхнім дешифруванням. За справу взялися Джон Хассард і Вільям Гросвенор, економічний оглядач «*The New York Tribune*». Причому Хассард працював над криптограмами настільки завзято, що застудився, занедужав туберкульозом і наступні останні десять років свого життя думав лише про своє одужання.

Пізніше Рейд згадував: «Обоє вони трудилися надзвичайно добре, працювали незалежно один від одного, чесно порівнюючи результати, чудово співробітничали разом… Хассард трохи раніше почав працювати в цій сфері та заслужив особливої похвали. Гросвенор був також здібним і, як я зараз пригадую, досяг майже такого ж успіху. Іноді він і Хассард підходили до дешифрування однієї і тієї ж криптограми з різних боків і після кількаразових невдач, нарешті, знаходили вірне рішення в той самий вечір…»

Одночасно з Хассардом і Гросвенором над читанням криптограм, оприлюднених у редакційних статтях *«The New York Tribune»,* працював молодий математик з військо-

во-морської обсерваторії США у Вашингтоні Едвард Холден. У своїх мемуарах Холден написав з цього приводу: «До 7 вересня 1878 року я відкрив закономірність, за допомогою якої можна було безпомилково знайти будь-який ключ до найважчих і хитромудрих із цих телеграм». Він звернувся до газети «Нью-Йорк трибюн», якій сподобалася ідея найняти професійного математика. Хассард вислав Холдену велику кількість криптограм. Однак на той час Хассард і Гросвенор незалежно від Холдена розробили свої криптоаналітичні методи та зуміли випередити його в читанні деяких криптограм. Рейд стверджував, що жодної з дешифрованих Холденом криптограм «The *New York Tribune*» не одержала раніше, ніж ці ж самі криптограми були прочитані Хассардом і Гросвенором. Тому результати роботи Холдена розглядалися лише як підтвердження правильності дешифрувань Хассарда і Гросвенора.

Результат перевершив усі сподівання. Громадськість була обурена з приводу непорядності демократів і захоплена винахідливістю дешифрувальників. Тисячі читачів розшифровували криптограми за допомогою ключів, опублікованих у «*The New York Tribune*», із задоволенням відзначали правильність їхнього розшифрування. До того ж до виборів у Конгрес залишалося усього кілька тижнів. На них республіканці здобули значну перемогу.

Частина дешифрованих телеграм була на адресу Тілдена – його племіннику У. Пептону. І хоча Тілден клявся, що

зовсім не знав, чим займався його племінник і що все було зроблено без його дозволу, репутація Тілдена була назавжди заплямована. Це викриття поклало кінець його надіям стати президентом. Навіть біограф Тілдена, що мав до нього велику симпатію, визнав, що в результаті дешифрування телеграм демократів республіканці одержали перевагу, яка забезпечила їм перемогу на президентських виборах у 1880 році. Ось так криптоаналіз допоміг обрати американського президента.

У листопаді 1899 року «червоний» шифр Держдепартаменту був замінений на новий – «блакитний» (англ. *blue),* який знову був розроблений Джоном Хасвелом і названий за кольором своєї обкладинки. Книга була більш докладною, містила найбільш уживані терміни та фрази з кореспонденції посольств і консульств, тому мала вже 1500 сторінок. Для підвищення стійкості свого коду Хасвел розробив також «Доповнення до шифру Держдепартаменту: код, що не піддається декодуванню» на 16 сторінках. У цьому доповненні перераховувались додатково ще 25 правил, або способів перешифрування, які могли застосовуватися до закодованих повідомлень, крім вказаних у доповненнях до «червоного» шифру.

У 1910 році Держдепартамент прийняв на озброєння «зелений шифр» (англ. *green),* який складався з двох частин (кодування і декодування) і мав 1418 сторінок. У березні 1918 року був введений в дію «сірий» (англ. *grey)* код, в яко-

му для позначення стандартних термінів і фраз використовувались 5-буквені групи. У травні 1919 року «зелений шифр», який реально був тільки кодом, отримав відповідну йому назву «Код Держдепартаменту А-1». Ці коди разом використовувались американськими державними службовцями навіть до Другої світової війни, коли було потрібно здійснити зміни в дипломатичних і військових криптосистемах з метою підвищення їхньої стійкості. Так, наприклад, ще у 1940 році ще «сірим» кодом «закривалася» трансатлантичне листування, навіть між керівниками США і Британії.

30 грудня 1937 року був введений в дію «коричневий» (англ. *brown)* код Держдепартаменту, який містив розділ для кодування обсягом 954 сторінки та розділ для декодування обсягом 938 сторінок. Подібно «*А-1*» та іншим сучасним на той час кодам «коричневий» код мав багаточисельні варіанти заміни для часто уживаних слів. Він також поклав початок системі кодування дат і часу, що стало нововведенням наприкінці 1930-х років. Місяці позначалися першою буквою, дні – другою та третьою, час – четвертою, а за допомогою п'ятої букви уточнювалася половина дня – перша чи друга. І хоча цей код у 1939 році був викрадений з американського консульства у Загребі (Югославія), ним продовжували користуватися навіть під час Другої світової війни.

Кодом американських військових атташе у той час був «чорний» (англ. *black),* отримавший назву за кольором своєї

палітурки. На початку 1940 року він вважався невразливим, оскільки додаткову стійкість йому забезпечували шифрувальні таблиці. Але насправді вже на початку війни він був скомпрометований: його «зламала» німецька служба радіоперехвату та криптоаналізу.

2. Винахід «лінійного» шифрування

В історії криптології спрощення процедури ручного шифрування шляхом механізації цього процесу здавна цікавило багатьох фахівців. Допитливі розуми винахідників неодноразово намагалися вирішити цю проблему. Спроб було багато, але лише деякі змогли залишити в історії помітний слід і закласти фундамент для майбутньої механізації, а потім і автоматизації шифрувальної справи.

Поштовхом до необхідності автоматизувати процес шифрування послужили технічні досягнення кінця XIX століття, такі як телеграф, телефон і радіо, при використанні яких для передачі криптограм удалося істотно підвищити оперативність шифрованого зв'язку. Слідом за змінами у зв'язку змінювалася й криптологія, яка стала спочатку електромеханічною, а потім електронною. Швидкість передачі інформації дуже зросла та все більші обсяги її були піддані перехопленню та прочитанню. Шифрувальники, що вручну заміняли букви та склади спеціальними символами, уже не могли упоратися з постійно зростаючим потоком інформації.

Радіозв'язок виявився дешевшим та мобільнішим за проводовий. З'явилася можливість активізувати повідомлення між військовими підрозділами, установлювати зв'язок з рухомими об'єктами (автомобілями, літаками, кораблями). Однак при цьому спростилося перехоплення переданих та-

ким чином повідомлень, що, зокрема, підтвердила практика Першої світової війни.

Незважаючи на те, що всі учасники бойових дій постійно розробляли нові коди та вдосконалювали старі, забезпечити їхнє збереження вдавалося далеко не завжди. В результаті супротивники нерідко були цілком поінформовані про все, що було в таємному листуванні ворога. З цим були пов'язані і деякі трагічні події, з яких згадаємо у третій частині лише розгром двох російських армій – Раненкампа та Самсонова в Східній Пруссії в серпні 1914 року. Причиною їхнього розгрому була погана організація «закритого» зв'язку, у результаті чого переговори по радіо велися взагалі без усякого шифрування.

Під час війни головним (і найчастіше єдиним) засобом засекречування було кодування. Коди часто застосовували не тільки для того, щоб забезпечити таємність переданої інформації, але й щоб скоротити довжину повідомлення або зробити його більше зрозумілим. Найчастіше код являв собою набір символів (цифр або букв), що заміняли конкретні назви.

До речі, розвиток технічного шпигунства й, зокрема, радіоперехоплення, буквально ні на крок не відставав від розвитку систем передачі повідомлень, освоюючи нові діапазони та способи модуляції. Проте основна маса телеграфних та телефонних повідомлень передавалася або після їх закриття шифрами простої заміни, або просто відкритим текстом.

Різке розширення обсягів зашифрованих передач і порівняльна простота радіоперехоплення повідомлень підштовхнули дешифрувальників до думки про те, що дослідження окремої перехопленої криптограми необхідно зв'язати з аналізом усього масиву перехоплення, у якому з'явилася ця криптограма. Цей шлях виявився досить плідним. Як справедливо відзначає Д. Кан, «телеграф створив сучасну шифрувальну справу, радіо – сучасний криптоаналіз».

Шифрований текст, переданий по радіо, був доступний кожному, хто мав у своєму розпорядженні нескладний приймач. І навіть, якщо цей текст не можна було розшифрувати відразу, його можна було використовувати при аналізі наступних повідомлень. У цей період одержали розвиток методи дешифрування, засновані на парах відкритих і шифрованих текстів; на декількох шифровках, створених за допомогою одного ключа; на переборі ймовірних ключів. Саме ці методи застосовувалися англійцями для читання секретного листування німців під час Першої світової війни.

Телеграф і радіо почали поступово витісняти кодування з метою захисту інформації на користь застосування шифрів. Громіздкі та малозручні при використанні секретні кодові книги могли стати і ставали здобутком супротивника, а їхня зміна породжувала серйозні проблеми. Шифри виявилися набагато мобільнішими та дешевшими. Секретне кодування почало зменшуватися, але не зникло зовсім. Коди стали застосовуватися разом із шифрами. Таке сполучення

виявилося досить ефективним і дійшло до наших днів. Підкреслимо, що при компрометації шифру досить лише змінити його ключі, а не всі кодові книги. Відзначимо також, що коди дуже чуттєві до лексики та словникового запасу мови спілкування. Поява нових термінів і понять приводила до необхідності поновлення кодових книг. Шифри в цьому плані набагато важливіші, тому що їхнє застосування не пов'язане зі змістом відкритого тексту.

До речі, у 1881 році була запатентована перша ідея телефонного шифратора Д.Х.Роджерсом. Ідея складалася в передачі телефонного повідомлення декількома (у найпростішому випадку – двома) лініями за допомогою почергових імпульсів у деякій послідовності, яка швидко змінювалася та нагадувала телеграфне повідомлення. Пропонувалося рознести такі лінії на значну відстань одна від одної для того, щоб усунути можливість підключення відразу до всіх одночасно. Підключення ж до однієї з них дозволяло б чути лише окремі нерозбірливі сигнали.

У XIX столітті застосовувалося, в основному, так зване, попереднє шифрування повідомлень. У цьому випадку відправник зашифровував передане повідомлення (у якому шифротекст задовольняв вимогам телеграфної передачі), після чого відносив шифроване повідомлення на телеграф. У XX столітті таке уповільнення в передачі повідомлень часто виявлялося неприйнятним. Треба було розробити методи так званої лінійної передачі шифрованих повідомлень,

при якій апарат шифрування (шифратор) знаходився би безпосередньо в апаратурі передачі послань. Таким чином, передача шифрованого повідомлення в принципі не відрізнялася би від передачі нетаємного повідомлення.

Таку ідею автоматичного шифрування телеграфних повідомлень у грудні 1917 року запропонував американець Жильбер Вернам (1890—1960), молодий інженер компанії «Американський телефон і телеграф» (англ. *American telephone and telegraph, AT&T)* та талановитий винахідник. Він працював у телеграфному відділенні науково-дослідного відділу компанії, де займалися розробкою «телетайпу» – букводрукуючого телеграфного апарату.

Ще влітку, через кілька місяців після того, як Сполучені Штати оголосили війну Німеччині, в компанії почалася робота над секретним проектом щодо можливості зберігання в таємниці повідомлень, переданих телетайпом. Під час досліджень виявилося, що коливання струму в лінії зв'язку могли бути записані за допомогою осцилографу та потім легко перетворені в букви переданого повідомлення. Тому було вирішено внести зміни в з'єднання дротів друкуючого механізму телетайпу. У результаті текст повідомлення шифрувався методом одноалфавітної заміни. У телеграфному відділенні розуміли, що такий захист був занадто слабким, однак нічого іншого придумати не змогли та припинили займатися цією проблемою до тих самих пір, поки Вернам не повідав їм про свою ідею.

Він запропонував використовувати особливості телетайпного коду Бодо, в якому кожний знак складався з п'яти елементів. Кожний з цих елементів символізував наявність (»+») чи відсутність (» —») електричного струму в лінії зв'язку. Таким чином, було 32 різні комбінації «+» і «—». 26 з них повинні були відповідати буквам, а ті, що залишилися, позначали «службові комбінації» (пробіл між словами, перехід з букв на цифри та розділові знаки, зворотний перехід з цифр і розділових знаків на букви, повернення каретки друкуючого пристрою, перехід на новий рядок і холостий хід).

Наприклад, буква «А» позначалася комбінацією «++–», а перехід на цифри та розділові знаки позначався комбінацією «++—++». Закодоване повідомлення набивалося на перфострічці: «+» були дірками, а «—» – їхньою відсутністю. При зчитуванні перфострічки металеві щупи проходили через дірки, замикали електричне коло та посилали імпульси струму по дротах. А там, де на перфострічці знаходився «—», папір не дозволяв цим щупам замкнути коло, і в результаті струмовий імпульс не передавався.

Вернам запропонував готувати перфострічку з випадковими знаками (так звану «гаму») заздалегідь і потім електромеханічно складати її імпульси з імпульсами знаків відкритого тексту. «Гама» – це секретний ключ, що хаотичним набором букв того ж самого алфавіту. Отримана сума являла собою шифротекст, призначений для передачі по лінії

зв'язку. Вернам установив таке правило підсумовування: якщо відразу обидва імпульси були «+» чи «—», то підсумковий імпульс буде «-», а якщо ці імпульси різні, то в результаті вийде «+».

Додавання, за сучасною термінологією, здійснюється «за модулем 2» («0» означає знак «—», а 1 – «+»): 0 +0 = 0; 0 +1 = 1; 1 +0 = 1; 1 +1 = 0. Нехай, наприклад, знак «гами» має вигляд: «+—+–» (10100). Тоді буква «А» – «+ +–» (11000) при шифруванні переходить у двійкову комбінацію «—++–»: (01100) = (11000) x (10100). При розшифруванні ту ж операцію необхідно повторити у зворотному порядку: (01100) x (10100) = (11000) – «++–» – буква «А».

Щоб підсумовувати електроімпульси при шифруванні, Вернам сконструював спеціальний пристрій, що складався з магнітів, реле та струмознімних пластин. А оскільки процедура розшифрування була аналогічна процедурі зашифрування, цей же прилад міг бути використаний і при розшифруванні. Імпульси надходили в пристрій підсумовування з двох зчитувачів: один зчитував «гаму», а інший – відкритий текст. «Плюси» й «мінуси», що отримували на виході, можна було передавати як звичайне телетайпне повідомлення. На прийомному кінці пристрій, винайдений Вернамом, додавав імпульси, що зчитувалися з ідентичної стрічки з «гамою», і відновлював вихідні імпульси відкритого тексту.

Важливість винаходу Вернама полягала в тому, що більше не потрібно було здійснювати зашифрування й розшиф-

рування секретних повідомлень у вигляді окремих операцій. Відкритий текст входив в апарат, що знаходився у відправника повідомлення, і такий же відкритий текст виходив з апарата, що належав одержувачу цього повідомлення. А якщо хто-небудь перехоплював це повідомлення на шляху проходження від відправника до одержувача, то в його розпорядженні виявлялася нічого не значуща послідовність «плюсів» і «мінусів». Тепер, щоб зашифрувати, передати, прийняти та розшифрувати повідомлення, було потрібно прикласти не набагато більше зусиль, ніж при відправленні повідомлення відкритим текстом.

Основна перевага винайденого Вернамом методу засекречування повідомлень полягала не в механічному шифруванні відкритого тексту з наступною печаткою результату на папері, що було здійснено ще на початку 70-х років XIX століття французами Емілем Вінеєм і Жозефом Госсеном. Вернам уперше зумів поєднати два процеси – шифрування та передачу повідомлення. Він створив те, що згодом назвали лінійним шифруванням, щоб відрізняти його від традиційного попереднього шифрування. Вернам звільнив процес шифрування від кайданів часу й помилок, виключивши з цього процесу людину. Видатний внесок, зроблений Вернамом у практику шифрування, полягає саме в тому, що він привніс у шифрувальну справу автоматизацію, що вже встигла до початку XX століття послужити людям у багатьох сферах їхньої діяльності.

Навколо ідеї, висловленої Вернамом у колі колег, моментально розгорнулася активна діяльність. Спочатку Вернама змусили викласти цю ідею в короткій записці, яка була датована 17 грудня 1917 року. Компанія *«AT&T»* повідомила про винахід Вернама американське військово-морське відомство, з яким вона підтримувала тісне співробітництво. 18 лютого 1918 року відбулася нарада, у якій взяли участь Вернам і інші інженери з телеграфного відділення компанії *«AT&T»,* з одного боку, і військові моряки, з іншого.

27 березня ці ж інженери зустрілися зі своїми колегами з американської компанії «Вестерн електрик», виробничої філії «*AT&T*», і домовилися з ними про виготовлення перших двох лінійних шифраторів із використанням якомога більшої кількості стандартних деталей. У лабораторії «Вестерн електрик» виготовлені шифратори були приєднані до телетайпів і здійснені перші іспити процесу, що назвали «автоматичним шифруванням». Усі пристрої, що входили до його складу, працювали без збоїв. Компанія *«AT&T»* проінформувала про цей факт майора Джозефа Моборна (1881—1971), що займав тоді посаду начальника відділу науково-дослідних і конструкторських розробок військ зв'язку Армії США.

Невирішеним залишалося всього одне питання – звідки брати «гаму». Спочатку «гама» для пристрою Вернама являла собою склеєні петлею короткі перфострічки, на які були набиті знаки, витягнуті навмання з різних відкритих текстів.

Інженери компанії *«AT&T»* майже відразу звернули увагу на істотні вади такого процесу «автоматичного шифрування», пов'язані з недостатньою довжиною «гами». Тому, щоб ускладнити криптоаналіз, вони зробили перфострічки з «гамою» більш довгими. Але тоді ці перфострічки стало занадто важко використовувати.

Вернам запропонував підсумовувати дві короткі, що мають різну довжину «гами» таким чином, начебто б одна «гама» шифрувала іншу. Отримана в результаті так звана вторинна «гама», яка мала значно більшу довжину, ніж дві вихідні первинні «гами», що були використані для її генерації, була застосована для зашифрування відкритого тексту. Наприклад, якщо одна закільцьована стрічка мала 1000 знаків, а інша – 999, то дане розходження в довжинах усього в один знак давало 999 000 комбінацій, перш ніж результуюча послідовність повторювалася.

Однак Моборн розумів, що навіть удосконалена система Вернама дуже вразлива для криптоаналізу. У свої 36 років майбутній начальник військ зв'язку США Моборн був неабияким криптоаналітиком. Він ґрунтовно вивчив криптоаналіз в армійській школі зв'язку та був добре обізнаний з останніми досягненнями в цій сфері. Більш того, за кілька років до описуваних подій Моборн сам брав участь в одній науково-дослідній роботі, у ході якої фахівці з армійської школи зв'язку зробили висновок про те, що єдиною стійкою «гамою» була така, що порівняна по довжині з самим пові-

домленням. Будь-яке повторення в «гамі» піддавали величезному ризику отримані за її допомогою криптограми та, скоріше за все, привели би до їх розкриття.

Проведений Моборном аналіз системи «автоматичного шифрування» ще більше переконав його в цьому. Він зрозумів, що не має ніякого значення, чи знаходяться повторення в межах однієї криптограми чи вони розподілені по декількох, чи виходять вони шляхом комбінування двох первинних «гам», чи в результаті простого повторення в єдиній довгій «гамі». Важливим було те, що в «гамі» повторень не повинно бути ні за яких умов. Необхідно, щоб вона була зовсім унікальна й максимально хаотична.

Усвідомивши це, Моборн об'єднав властивість хаотичності «гами», на що спирався Вернам у своїй системі «автоматичного шифрування», із властивістю унікальності «гами», виробленою криптографами армійської школи зв'язку, у системі шифрування, що нині прийнято називати «одноразовим шифроблокнотом». Одноразовий шифроблокнот містив випадкову «гаму», що використовувалася тільки одного разу. При цьому для кожного знака відкритого тексту передбачалося використання абсолютно нового знака «гами», який не піддавався прогнозуванню.

Це була стійка шифросистема. Переважна більшість систем шифрування були абсолютно стійкими лише на практиці, оскільки криптоаналітик міг знайти шляхи їхнього розкриття при наявності в нього визначеної кількості шифро-

тексту та достатнього часу для його дослідження. Одноразовий же шифроблокнот був абсолютно стійким як у теорії, так і на практиці. Яким би довгим не був перехоплений шифротекст, скільки б багато часу не приділялося на його дослідження, криптоаналітик ніколи не зможе розкрити одноразовий шифроблокнот, використаний для одержання цього шифротексту. І ось чому.

Розкриття багатоалфавітного шифру означало об'єднання всіх букв, зашифрованих за допомогою одного шифроалфавіту, у єдину групу, яку можна вивчати на предмет виявлення її лінгвістичних особливостей. Методи такого об'єднання могли бути різними в залежності від виду «гами». Так, метод Казиського полягав у виділенні ідентично «гамованих» букв відкритого тексту при повторюваній «гамі». Зв'язна «гама» могла бути розкрита шляхом взаємного відновлення відкритого тексту та «гами». А «гама», використана для зашифрування двох чи більше повідомлень, піддавалася розкриттю шляхом одночасного відновлення відкритих текстів цих повідомлень, причому правильність прочитання одного тексту контролювалася читаністю іншого. Майже для всіх різновидів багатоалфавітних шифрів був розроблений свій метод розкриття, заснований на їхніх відмінних рисах.

Зовсім іншою була ситуація з одноразовим шифроблокнотом. У цьому випадку криптоаналітик не мав відправної крапки для своїх досліджень, оскільки в одноразовій шифросистемі «гама» не містила повторень, не використовува-

лася більше одного разу, не була зв'язним текстом і не мала внутрішніх структурних закономірностей. Тому всі методи дешифрування, тією чи іншою мірою засновані на цих характеристиках, не давали ніяких результатів. Криптоаналітик заходив до тупика.

Залишався лише метод тотального випробування. Адже прямий перебір усіх можливих ключів, у кінцевому рахунку, обов'язково приводив криптоаналітика до відкритого тексту. Однак успіх, досягнутий цим шляхом, був ілюзорним. Тотальне випробування дійсно дозволяло одержати вихідний відкритий текст. Але воно також давало й кожен інший можливий текст тієї ж довжини, тому сказати, який з них є правильним, було неможливо.

Разом із тим, цей досконалий шифр не знайшов широкого застосування через величезну кількість «гам», що потребуються при його використанні. Проблеми, що виникають при виготовленні, розсиланні та знищенні «гами», людині, не обізнаній в усіх тонкощах організації шифрозв'язку, можуть здатися дріб'язковими, однак у воєнний час обсяги листування стають дуже великими. Протягом доби може знадобитися зашифрувати сотні тисяч слів, а для цього потрібно виготовити мільйони знаків «гами». І оскільки «гама» для кожного повідомлення повинна бути єдиною та неповторною, то її загальний обсяг буде еквівалентний обсягу всього листування за час війни.

Таким чином, практичні проблеми не дозволили застосо-

вувати одноразові шифроблокноти у ситуаціях, які швидко змінюються, наприклад, у ході проведення військових операцій. Цих проблем не існувало в більш стабільних умовах: у генеральних військових штабах, дипломатичних представництвах або агентурному листуванні одноразові шифроблокноти були досить практичними та знайшли застосування. Однак і тут виникали нездоланні труднощі, якщо обсяг листування був занадто великим.

Це саме й відбулося, коли Моборн, улаштувавши перший великий іспит шифросистеми Вернама, установив його машини відразу в трьох містах. Навіть, при порівняно невеликому обсязі листування (до 135 коротких повідомлень щодня) виявилося неможливим виготовити достатню кількість якісної «гами». Тому, не знайшовши іншого виходу зі скрутного становища, Моборн став комбінувати з двома відносно короткими «гамами» з метою одержання з них більш довгої «гами», як це спочатку й пропонував робити сам Вернам.

У вересні 1918 року Вернам відправився до Вашингтона та подав там заявку на патент. Перша світова війна встигла закінчитися скоріше, ніж шифросистема Вернама зуміла хоч якось виявити свої достоїнства на практиці. Проте 22 липня 1919 року на неї був виданий патент №1310719 – найважливіший в історії криптології. Експерти з вашингтонського патентного бюро визнали можливу корисність цього винаходу й у мирний час.

Хоча прилад, утворений Вернамом, безсумнівно був цін-

ним результатом творчої інженерної думки талановитого винахідника, у комерційному плані він зазнав повного «провалу». Телеграфні компанії та комерційні фірми, що, на думку «AT&T», повинні були масово закуповувати запатентовані шифроприставки Вернама до своїх телетайпів, віддавали перевагу старомодним кодам, що істотно знижували довжину повідомлень, тим самим зменшуючи телеграфні витрати й одночасно забезпечуючи хоч якусь, навіть невелику, безпеку листування. Після закінчення Першої світової війни бюджети збройних сил усіх країн були скорочені до мінімуму. Недолік засобів і недостатність матеріальних ресурсів змусили армійських зв'язківців знову повернутися до комбінування двох відносно коротких стрічок з «гамою», а продемонстрована військовими криптоаналітиками слабка стійкість такої системи генерації «гами» призвела до того, що шифросистема Вернама на якийсь час була забута.

Стосовно ж самого Вернама, то він продовжував займатися науково-дослідною роботою в компанії «AT&T». Учений удосконалив свою шифросистему, а також винайшов прилад для автоматичного шифрування написаного від руки тексту під час його передачі фототелеграфом. У 1929 році Вернама зі значним підвищенням перевели в одну з філій компанії «AT&T». Однак через чотири місяці в США вибухнула фінансова криза, і, оскільки Вернам ще не встиг заробити достатній виробничий стаж на новому місці, його незабаром звільнили. Він перейшов на роботу в іншу велику компанію,

але різка зміна в його особистій долі, певно, подіяла на нього гнітюче. З кожним роком про Вернама було чути усе менше і менше, поки нарешті 7 лютого 1960 року людина, що автоматизувала процес шифрування, не вмерла практично в повному забутті.

3. «Чорний кабінет» Ярдлі

У 1912 році у Держдепартаменті у якості шифрувальника почав працювати Герберт Ярдлі (1889—1958), один із видатних американських криптоаналітиків. На початку своєї кар'єри Ярдлі звернув увагу на слабкість шифрів, які використовувались американським урядом. Він був приголомшений, дізнавшись, що президент Вудро Вільсон користується кодом, який використовується впродовж більше 10 років. Так, коли Президенту США Вудро Вільсону було передане закодоване повідомлення з 500 слів від його радника Хауза, Ярдлі був уражений тим, що прочитав це повідомлення усього за кілька годин.

Досягнутий успіх ще більше підвищив інтерес Ярдлі до криптоаналізу, і він У травні 1916 року написав 100-сторінковий меморандум «Розкриття американських дипломатичних кодів», який передав своєму керівництву. Заглибившись у проблему можливого розкриття чергового коду, він першим поставив діагноз явищу, що з тих пір відомо серед американських криптоаналітиків як «симптом Ярдлі»: «Просинаючись, я відразу починаю про це думати. Засинаючи, я все одно продовжую думати про це».

6 квітня 1917 року американський Конгрес оголосив про вступ США у Першу світову війну проти Німеччини. А 28 квітня у складі Управління військової інформації

«MID» (англ. *Military Information Division)* Генштабу Військового департаменту (англ. *War Department General Staff)* була створена кабельно-телеграфна секція (англ. *Cable and Telegraph Section),* яка отримало кодову назву *«MI-8»* (англ. *Military Information, Section* 8).

Для участі в бойових діях Першої світової війни на територію Франції було перекинуто морем експедиційне з'єднання американських військ під командуванням генерала Джона Першинга чисельністю більше 175 тисяч осіб. Ярдлі був направлений в Американський експедиційний корпус у якості офіцера-шифрувальника. Вже в перші місяці роботи Ярдлі на практиці продемонстрував свої видатні криптоаналітичні здібності. Участь у війні дала йому можливість переконати «батька» американської військової розвідки «MID» майора Ральфа ван Демана в необхідності створити спецпідрозділ для «злому» шифрів інших країн. Він домігся успіху не тільки тому, що американській армії були потрібні криптоаналітики, але й завдяки винятковому таланту переконувати людей у своїй правоті. В результаті у червні 1917 року Ярдлі у званні другого лейтенанта вже очолив *«MI-8».*

Навчальний підрозділ *«MI-8»,* що займався підготовкою криптоаналітиків, очолив доктор Джон Менлі. 52-літній філолог, який був деканом факультету англійської мови в Чиказькому університеті, а також давнім і палким шанувальником криптоаналізу, Менлі став одним з кращих крипто-

аналітиків *«MI-8»*. Очолюваний ним підрозділ був розташований та проводив заняття з криптоаналізу у військовому коледжі армії США.

«MI-8» читала дипломатичне шифролистування Аргентини, Бразилії, Німеччини, Іспанії, Коста-Рики, Куби, Мексики, Панами і Чилі. Служба американської цензури надсилала до *«MI-8»* перехоплені шифровані листи. Більшість із них на перевірку виявлялася любовними посланнями, у яких застосовувалися дуже прості шифри. Хоча багато з них були настільки компрометуючими, що Ярдлі часто повторював: «Мене дратує той факт, що чоловіки й дружини довіряють своє таємне листування таким слабким методам шифрування».

Найважливіша з розробок *«MI-8»* привела до звинувачення Лотара Вітцьке -єдиного німецького шпигуна, засудженого в США до страти під час Першої світової війни. 25 січня 1918 року при обшуку в його багажі був виявлений шифрований лист, датований 15 січня. Він потрапив до *«MI-8»* тільки навесні і пробув там протягом ще декількох місяців, поки криптоаналітики безуспішно намагалися його дешифрувати. Зрештою цей лист вдалося прочитати Менлі, який у з'ясував, що він був надісланий німецьким послом у Вашингтоні Еккардтом німецькому консулу в Мексиці. Відкритий текст листа був таким:

«Пред'явник цього є підданим Німецької імперії, що подорожує під ім'ям Павла Ваберського. Він є німецьким сек-

ретним агентом. Якщо він звернеться до вас із проханням, будь ласка, забезпечте йому захист і надайте допомогу. Також видайте йому до тисячі песо золотом і посилайте його шифровані телеграми до нашого посольства в якості офіційних консульських депеш».

Коли Менлі зачитав цей текст у залі суду на закритому процесі за обвинуваченням Вітцьке в шпигунстві, сумнівів у його винності ні в кого не залишилося. Шпигун був засуджений до страти через повішення. Однак Вільсон замінив смертний вирок довічним ув'язненням. У 1923 році Вітцьке був помилуваний та випущений на волю.

9 лютого 1918 року *«MID»* було реорганізоване в Управління військової розвідки (англ. *Military Intelligence Division).* У листопаді того ж року *«MI-8»* нараховувала 18 офіцерів, 24 цивільних криптографів, 109 друкарок і стенографісток. Однак до травня наступного року її штатна чисельність скоротилася до 15 офіцерів, 7 цивільних криптографів і 55 технічних службовців.

Після участі Ярдлі в 1919 році в Паризькій мирній конференції в якості головного криптографа американської делегації керівництво розвідки оголосило про майбутнє згортання дешифрувальної роботи через утрату її актуальності. Ярдлі категорично заперечував і підготував доповідь під назвою «Вивчення та розкриття кодів і шифрів», у якій вказував, що Сполучені Штати мають досить ворогів у всьому світі, тому розкриття їхніх шифросистем дозволить уряду завчас-

но одержати інформацію про можливі загрози національній безпеці.

Ярдлі пропонував не припиняти цю роботу, а реорганізувати *«MI-8»* у криптослужбу мирного часу з подвійним підпорядкуванням Державного департаменту та Генштабу Військового департаменту. Ця аргументація настільки вразила начальника розвідки генерала Мальборо Черчиля, що він умовив держсекретаря зберегти «Бюро шифрів» і фінансувати його роботу з таємного фонду.

Це «Бюро шифрів», що пізніше стало відомим як «американський чорний кабінет» (англ. *american black chamber)* (далі – АЧК), повинно була спільно фінансуватися двома департаментами на суму приблизно в 100 000 доларів у рік, але її фактичні витрати ніколи не досягали цієї суми. За законом платежі Держдепартаменту, що почали надходити в червні 1919 року, не могли бути на законних підставах витрачені в межах Вашингтона, і тому Ярдлі разом з підібраним зі складу *«MI-8»* персоналом АЧК незабаром переїхав до Нью-Йорка. Військовим департаментом АЧК був уперше профінансований лише 30 червня 1921 року. Первісний бюджет Бюро склав 45 тисяч доларів замість запитаних 96 тисяч, а до 1929 року знизився до 19630 доларів.

Кінцевим продуктом криптослужби був бюлетень, що надсилався до Відділу військової розвідки та Держдепартаменту, у який включалися усі факти, що заслуговували уваги, природно, без посилань на справжнє походження інфор-

мації.

Усі повідомлення починалися стереотипно: «Із джерел, що заслуговують довіри, встановлено, що:». При цьому ніякого інформаційно-аналітичного підрозділу в «Бюро шифрів» не існувало, матеріали відбирав особисто його керівник, часто за суб'єктивними ознаками.

Післявоєнне дешифрування АЧК німецького листування базувалися на отриманих у Нідерландах у 1919 році ключах, що запропонував американським представникам ініціативник, відомий під агентурним псевдонімом «Дачмен». Як часто траплялося в подібних випадках, «Дачмена» обдурили: коли він залишив кодові таблиці для вивчення, їх сфотографували і повернули, нібито через непотрібність. На підставі його даних американці зуміли розкрити німецькі коди з позначеннями «2500», потім «2970», «9700», «5300» і «1219». Усього АЧК прочитав 20 німецьких кодів і шифрів, однак на післявоєнний період з них припало лише 9, що фактично являли собою варіації двох базових систем.

Одним з основних завдань, поставлених перед АЧК, було «розкриття» кодів Японії, напруженість у відносинах з якою зростала з кожним днем. У пориві ентузіазму Ярдлі пообіцяв домогтися їхнього «розкриття» протягом року або піти у відставку. Він пошкодував про свою обіцянку відразу, як тільки приступив до цієї справи, оскільки моментально заплутався у відкритих текстах японською мовою, не говорячи вже про самий шифротекст.

Після тривалого попереднього аналізу Ярдлі з'ясував, що для своїх телеграфних повідомлень, що передавалися буквами латинського алфавіту, японці використовували трохи видозмінену форму ієрогліфічної писемності, іменованої як «катакана». Але, незважаючи на ретельне вивчення перехоплених шифротелеграм, прочитати їх так і не вдавалося. Він писав:

«До цього часу я так довго працював з кодованими телеграмами, що кожен їхній рядок, навіть кожне кодове позначення назавжди викарбувалося в моїй голові. Я міг лежати на ліжку з відкритими очима та займатися своїми дослідженнями в повній темноті… І ось одного разу я прокинувся опівночі, тому що пішов з роботи рано, і звідкись із темряви прийшло переконання, що визначена послідовність двобук-вених кодових позначень повинна абсолютно точно відповідати слову „Ірландія“. Потім переді мною затанцювали, швидко змінюючись, інші слова – „незалежність“, „Німеччина“, „крапка“… Велике відкриття! Серце моє завмерло, я не міг рушити з місця. Чи було це зі мною уві сні або наяву, чи не зійшов я з розуму? Рішення? Нарешті, після всіх цих місяців! Я зістрибнув з ліжка та у поспіху (оскільки тепер уже точно знав, що не сплю) майже скотився по сходах. Тремтячими руками я відкрив сейф, схопив папку з паперами і квапливо почав робити замітки».

Протягом години Ярдлі перевіряв свої гіпотези, а потім, переконавшись, що початок успішному розкриттю покладе-

но, повернувся до себе додому та напився. Однак його радість була трохи передчасною. Ярдлі зустрівся з несподіваними труднощами, намагаючись підшукати перекладача з японської мови. Зрештою він знайшов добродушного місіонера, що у лютому 1920 року зробив для Ярдлі перші переклади відкритих текстів японських шифротелеграм. Через півроку місіонер-перекладач звільнився, усвідомивши шпигунський характер своєї праці. Однак на той час один із підлеглих Ярдлі зробив воістину нечуваний подвиг, вивчивши у цей термін дуже важку японську мову.

У 1920 році Ярдлі доповів про розкриття 4-х японських кодів, але це ствердження було не цілком коректним, оскільки розкриті системи були не кодами, а шифрами, причому досить невисокого рівня стійкості. Однак незабаром після цього «Бюро шифрів» дійсно досягло вражаючих успіхів. Усього з 1917 по 1929 роки американці зуміли скомпрометувати 31 японську шифросистему (умовні позначки від «*JA*» до «*JZ*» і від «*JAA*» до «*JJJ*») і прочитати 10000 текстів, 1600 з яких відносилися до Вашингтонської конференції. Це було дуже високим показником, особливо з урахуванням гострої нестачі співробітників зі знанням мови.

Улітку 1921 року АЧК прочитав японську шифротелеграму від 5 липня, яка була направлена до Токіо послом Японії в Лондоні та містила перші згадування про конференцію з роззброєння, що повинна була відбутися в листопаді у Вашингтоні. Після цього читання японського дипло-

матичного шифролистування стало настільки регулярним, що за кілька місяців до відкриття конференції були введені щоденні поїздки кур'єрів між АЧК і Держдепартаментом. Одна офіційна особа в уряді США з посмішкою помітила, що керівники Держдепартаменту відносилися до роботи криптоаналітиків з АЧК із замилуванням і щоранку читали дешифровані ними японські криптограми, попиваючи при цьому апельсиновий сік або каву.

Метою Вашингтонської конференція з роззброєння було обмежити тоннаж великих військових кораблів. По мірі того, як переговори наближалися до свого головного результату – договору п'яти держав, який встановлював визначене співвідношення тоннажу для Англії, Італії, США, Франції і Японії, персонал Ярдлі читав усе більшу кількість секретних шифрованих інструкцій, що призначалися для країн, що брали участь у переговорах. Він писав: «Американський чорний кабінет, глибоко захований за надійними запорами, усе бачить й усе чує. Хоча віконниці закриті й вікна ретельно зашторені, його гострий зір спостерігає за тим, що діється на секретних нарадах у Вашингтоні, Женеві, Лондоні, Парижі, Римі і Токіо. Його чутливі вуха чують навіть найслабший шепіт у столицях іноземних держав».

Кожен учасник переговорного процесу у Вашингтоні прагнув домогтися найбільш сприятливого для себе тоннажного співвідношення. Найагресивнішою виявилася Японія, що виношувала широкомасштабні задуми, пов'язані з екс-

пансією в Азії, але побоювалася викликати невдоволення своїми діями з боку США. У самий розпал конференції, коли Японія зажадала встановити для себе співвідношення 10 до 7 у порівнянні зі США, АЧК прочитав японську шифротелеграму від 28 листопада, яку Ярдлі пізніше назвав найважливішою з дешифрованих ним криптограм.

«Вам слід подвоїти зусилля для досягнення поставлених цілей відповідно до проведеної нами політики, уникаючи при цьому будь-яких зіткнень з Америкою з питання про обмеження озброєнь, – телеграфувало японське МЗС своєму послу у Вашингтоні. – Ви повинні домогтися прийняття пропозиції про співвідношення тоннажу 10 до 6,5. Якщо ж, незважаючи на всі ваші зусилля, через сформовану ситуацію й у інтересах нашої політики виникне потреба піти на поступки, вам необхідно заручитися згодою всіх сторін на обмеження права концентрації Військово-морських сил і проведення маневрів на Тихому океані в обмін на нашу гарантію зберегти там статус-кво. У прийнятій угоді вам також варто зробити відповідне застереження, з якого було б зрозуміло, що саме в цьому складається наш намір, коли ми приймаємо співвідношення 10 до 6».

Зменшення тоннажу Військово-морських сил Японії на 0,5 умовних одиниць, про що йшла мова в цій японській шифротелеграмі, приблизно відповідало двом великим бойовим кораблям. Оскільки представники США на переговорах вчасно одержали з АЧК інформацію про те, що у ви-

падку натиску японці погодяться на збільшення тоннажного співвідношення між Америкою і Японією, залишалося тільки зробити цей натиск на практиці. Що і зробив держсекретар Чарльз Х'юз.

10 грудня Японія «капітулювала». У шифротелеграмі, яка була прочитана АЧК, японська делегація на переговорах у Вашингтоні отримала інструкцію з Токіо про те, що необхідно прийняти співвідношення, запропоноване США. У результаті договір, підписаний п'ятьма державами, встановив для США та Японії співвідношення тоннажа великих військових кораблів у розмірі 10 до 6. Японці сподівалися на більше. Однак домогтися бажаного їм перешкодив АЧК.

За час проведення конференції в АЧК було прочитано та перекладено більше 5000 шифроповідомлень. Внаслідок перенапруження декілька його співробітників занедужали на нервовому ґрунті: один почав щось незв'язно бурмотіти, інший став присвячувати весь свій вільний час ловлі бродячого собаки, у якого на боці нібито був записаний японський дипломатичний код, а третьому уявлялися жахіття, і він постійно носив при собі величезну сумку з камінням, зібраним на морському березі. В результаті усі троє були змушені піти з роботи. Сам Ярдлі також виявився на межі нервового розладу та у лютому 1922 року одержав чотиримісячну відпустку для відновлення свого здоров'я.

Крім стану здоров'я співробітників, предметом постійної турботи з боку держави стало також забезпечення безпеки

функціонування АЧК. Його пошта направлялася на підставну адресу. Прізвище Ярдлі не значилося в телефонному довіднику міста Нью-Йорк. Замки на дверях мінялися якнайчастіше. Проте відомості про діяльність АЧК усе-таки просочилися за кордон, тому що була здійснена спроба підкупити Ярдлі. Коли вона провалилася, на службове приміщення АЧК був зроблений напад, після якого зі столів зникли важливі документи.

Щоб не допустити нової пропажі, були прийняті додаткові заходи з безпеки. Тепер кожен аркуш паперу замикався на ніч у сейф, щоб нічого не залишалося в столах, хоча співробітникам АЧК усе-таки дозволялося брати додому матеріали, над розкриттям яких вони працювали.

Через якийсь час Ярдлі разом зі своїми підлеглими переїхав в інший службовий будинок. Як надійне прикриття для них була створена «Компанія зі складання кодів» (англ. *Code Compilation Company).* А щоб «легенда» виглядала цілком правдоподібною, Ярдлі склав «Загальний торгівельний код», яким компанія зі складання кодів стала торгувати разом з іншими розповсюдженими комерційними кодами.

У 1924 році асигнування АЧК були різко скорочені. У результаті Ярдлі довелося звільнити половину персоналу, і штат співробітників АЧК скоротився приблизно до 12 осіб. Однак, незважаючи на це, за словами Ярдлі, «у 1917—1929 роках АЧК вдалося прочитати більше 45 тисяч шифротелеграм Англії, Аргентини, Бразилії, Німеччини, Доміні-

канської Республіки, Іспанії, Китаю, Коста-Рики, Куби, Ліберії, Мексики, Нікарагуа, Панами, Перу, Сальвадору, Радянського Союзу, Франції, Чилі і Японії, а також проробити попередній аналіз багатьох інших кодів, включаючи коди Ватикану».

У 1929 році плідній діяльності АЧК зненацька прийшов кінець. Справа в тому, що до Ярдлі тексти іноземних шифротелеграм надходили від американських телеграфних компаній, які передавали їх йому з великим небажанням. Коли посаду Президента США зайняв Герберт Гувер, Ярдлі вирішив врегулювати питання про шифроперехоплення з новим урядом раз і назавжди. Він задумав зробити доповідь безпосередньо Президенту з викладом характеру діяльності АЧК, а також необхідних кроків, що повинні бути розпочаті, якщо уряд США бажає цілком використовувати майстерність своїх криптоаналітиків.

Після того як Генрі Стімсон, держсекретар при Гувері, пробув на своїй посаді кілька місяців, що, як вважав Ярдлі, було необхідно для придбання деякого досвіду практичної дипломатії, АЧК направив йому серію важливих дешифрованих криптограм. Однак на відміну від колишніх держсекретарів, на яких ця тактика завжди робила належний вплив, Стімсон, довідавшись про існування АЧК, обурився та суворо засудив його діяльність. Він обізвав її «підлим різновидом шпигунського ремесла» та розцінив як віроломне порушення принципу взаємної довіри, якого він неухильно до-

тримувався як у своїх особистих справах, так і у своїй зовнішній політиці.

Все сказане Стімсоном було справедливим, якщо, звичайно, відкинути точку зору, відповідно до якої будь-які засоби виправдані, коли вони корисні для інтересів батьківщини. Зробивши акт моральної мужності та припинивши усяку фінансову підтримку АЧК з боку Держдепартамента, Стімсон тим самим затвердив верховенство принципу над інтересами.

Оскільки гроші, що виділялися Держдепартаментом, складали головне джерело утримання АЧК, це означало його неминуче закриття. Невитрачені 6666 доларів і 66 центів, а також всі архіви АЧК були передані армійській службі зв'язку. Його співробітники швидко розбрелися хто куди (служити в армію ніхто з них не пішов), і 31 жовтня 1929 року АЧК *(МІ-8)* перестав існувати. Десять років його дешифрувальної роботи обійшлися американській скарбниці в 300 000 доларів, при цьому Державний департамент надав дві третини цієї суми, а Військовий – одну.

Ярдлі не зміг підшукати собі роботу і повернувся додому, в рідний Уортінгтон. Там він написав книгу «Американський чорний кабінет» на 375 сторінках, яка була надрукована 1 червня 1931 року. У книзі була викладена історія американської радіотехнічної розвідки та діяльності *«МІ-8»* під час Першої світової війни, а також АЧК у 1920-х роках і проілюстровані основні принципи радіорозвідки. Ця книга

відразу ж стала популярною.

Критики прийшли до висновку, що це був «найсенсаційніший внесок в таємну історію війни, а також післявоєнного періоду, який до цих пір не написана американцем». У США відразу ж було продано 17 931 примірників книги, 5480 – у Великобританії, вона була перекладена на французьку, шведську, японську і китайську мови. Японське видання вийшло безпрецедентним тиражем у 33119 примірників. Ця книга була неприємним сюрпризом для уряду США і скомпрометувала ряд джерел, використаних Ярдлі. Завдяки цій роботі 19 країн було попереджено, що їхні коди були «зламані».

«Батько» американської криптології Уільям Фрідмен, прочитавши книгу, «ошаленів», оскільки визнав, що Ярдлі розкрив джерела і методи роботи криптологів і непомірно прикрасив свої заслуги. Ярдлі, можливо, вважав, що публікація цієї книги змусить уряд відновити програми радіорозвідки, але добився прямо протилежного ефекту. Уряд США намагався почати судове переслідування Ярдлі, але він формально не порушив чинне законодавство відносно захисту урядових документів. До 1933 року були внесені поправки в Закон про шпигунство 1917 року, відповідно до яких було заборонено розкриття іноземних шифрів і шифрованих повідомлень. Друга книга Ярдлі «Японські дипломатичні коди, 1921—1922» була арештована та ніколи не публікувалася, а рукопис був розсекречений тільки у 1979 році.

Пізніше Ярдлі вступив на службу до китайського диктатора Чан Кайши з окладом 10 000 доларів у рік, щоб займатися дешифруванням японських криптограм. У 1940 році він повернувся з Китаю, щоб відправитися до Канади. Там Ярдлі організував дешифрувальне бюро. Однак незабаром його вислали назад до США, де у 1958 році він помер від серцевого нападу. Ще одна книга його мемуарів «Китайський чорний кабінет» (англ. *The Chinese Black Chamber)* була розсекречена та опублікована тільки у 1983 році.

За значний вклад у криптологію ім'я Герберта Ярдлі увічнене в Залі слави АНБ (англ. *NSA Hall of Honor)* та військової розвідки США (англ. *Military Intelligence Hall of Fame).* У бібліотеці Національного музею криптології США (англ. *National Cryptologic Museum)* зберігається 16 шаф із його особистими документами.

4. Армійська криптослужба

До початку Першої світової війни завдання забезпечення криптозахисту військових повідомлень у Армії США були покладені на три військові відомства:

1) Управління військової інформації «*MID*» Генштабу Військового департаменту відповідало за розробку армійських кодів і шифрів;

2) Генерал-ад'ютантський департамент (англ. *Army Adjutant General's Department)* забезпечував виготовлення кодових книг і шифродокументів та їхнє розсилання в підрозділи;

3) Війська зв'язку (англ. *Army Signal Corps)* відповідали за експлуатацію шифрувальної апаратури та забезпечення нею підрозділів армії. У той час на озброєнні Армії був кодовий диск, який був заснований на пристрої, зробленому Дж. Хіксом у Лондоні ще у 1893 році.

Підготовка фахівців з криптоаналізу для Армії США була розпочата за декілька років до початку Першої світової війни і спочатку здійснювалася у Школі військ зв'язку (англ. *Army Signal School),* розташованої у Форт-Лівенворт (штат Канзас). Пізніше всі питання, пов'язані з підготовкою таких фахівців, були передані у ведення *«MID».* Підготовка офіцерського і рядового складу почала здійснюватися у знов утвореній армійській школі криптології, яка розмістилася

в містечку Рівербенк, недалеко від м. Женева (штат Ілінойс). Керівництво школою було покладене на фахівця в області криптології полковника Джорджа Фабіана, якому вдалося привернути до викладання в школі ряд цивільних професорів і учених. Серед них був і Уільям Фрідмен, в подальшому один з керівників і провідних фахівців армійської криптослужби.

Під час Першої світової війни завдання з організації надійного та безпечного зв'язку частин американського експедиційного з'єднання у Франції, розробки та розсилки кодових книг і шифродокументів, а також керівництво підрозділами радіорозвідки з добування відомостей про супротивника були покладені на начальника зв'язку з'єднання бригадного генерала Едгара Рассела. Підпорядкований йому невеликий за чисельністю спеціальний підрозділ займався складанням польових кодів. Оформлені у вигляді таблиць коди призначалися для перетворення відкритих текстів команд, розпоряджень і донесень в еквівалентних їм умовні групи буквено-цифрових символів. Кодові книги, що розсилалися в бойові підрозділи, мали малий формат, були зручні для використання в польових умовах і містили близько 30 тисяч слів (фраз) і відповідних їм кодових значень.

Очолював ці роботи капітан Говард Барнс, що мав 10-річний досвід роботи з кодами Держдепартаменту. Уважно ознайомившись з існуючим британським кодом і вивчивши обстановку на полях битв, Барнс зі своїми помічниками

склав «Американський код для окопів». Цей код призначався для передачі повідомлень у роти діючої армії, проте дійшов він лише до штабів полків, оскільки існували побоювання, що його може захопити супротивник. Весною 1918 року була підготовлена та випущена 1 тисяча примірників «окопного» коду в паперовій обкладинці – книжечка поміщалася в нагрудній кишені.

У березні 1918 року було підготовлене та поширене 500 примірників книги телефонної коди. Він служив для приховування імен командного складу, офіцерів штабу і назв організацій. Спочатку передбачалося використовувати його тільки для телефонних переговорів, але він почав застосовуватися також і в інших засобах зв'язку. Оскільки для приховування змісту служив список жіночих імен, то дуже скоро він отримав прізвисько «Жіночий код».

24 червня 1918 року була введена в дію перша з кодових книг серії «Річкових кодів» – «Потомак». Це була книга на 47 сторінках, яка містила 1800 фраз і слів, складалася з двох частин і призначалася для використання в батальйонах. Спочатку було випущено 2 тисячі примірників. Як і у разі інших кодів, номер і час складання повідомлення, закодованого «Потомаком», передавалися відкритим текстом, але місце відправлення і адресат були закодовані. Повідомлення великого об'єму ділилися та пересилалися двома або декількома частинами.

Після «Суоні» та «Уобаша» четвертим з серії «Річкових

кодів» став «Мохаук». У серпні 1918 року було випущено для використання в батальйонах 3200 примірників кодової книги «Мохаук», що складалася з двох частин. Вона відрізнялася від своїх попередниць тим, що її коди складалися з груп по 4, а не по 3 цифри. У неї, як і у «Потомака», були варіанти для часто уживаних букв і чисел.

Роль експедиційного з'єднання американських військ зросла, коли в бойові дії вступила Друга армія. Для забезпечення захисту її зв'язку були розроблені коди, що отримали назву «Озерних кодів», тоді як Перша армія продовжувала користуватися діючим кодом «Колорадо» з серії «Річкових кодів». Назва коду «Шамплейн» на обкладинці була надрукована червоним кольором, щоб відрізнити його і наступні коди від «Річкових кодів», назви яких друкувалися чорним кольором. Цей код був триграфним і складався з двох частин.

У жовтні 1918 року був введений в дію другий з «Озерних кодів» – «Гурон». Цей код, що складався з двох частин, був примітний тим, що був першим в історії США кодом, призначеним для кодування телефонних переговорів у повному обсязі. Оскільки тепер до всього іншого ще і потрібно було забезпечити безпеку розмов по телефонах, які були украй уразливі для підслуховування, то для передачі відкритим текстом слів застосовувався фонетичний алфавіт. Такі слова вимовлялися по телефону по буквах, при цьому для приховування кожної букви використовувалися різні кодові

слова.

Також у жовтні був підготовлений та випущений «Американський службовий радіокод №1». Він складався з двох частин і приблизно 1 тисячі слів і фраз. 2 тисячі примірників книг з цим кодом було передано в бригади та артилерійські частини. Кодові групи були триграфи без варіацій. У 6 розділах частини, призначеної для кодування, були представлені типові, впорядковані за абеткою слова і фрази, серед яких були ті, що використовувалися при радіопередачах, а також словник з радіомереж та радіоапаратури.

Робота підрозділу була достатньо складною, особливо у разі компрометації кодів. Один з таких випадків відбувся з кодом «Потомак», який потрапив до рук німців через місяць після надходження кодових книг в підрозділи експедиційного з'єднання американських військ. У жовтні 1918 року те ж саме трапилося з кодом «Мохаук» і його наступником «Аллегейні». Було потрібно декілька діб напруженої роботи особового складу підрозділу для їх повної заміни. Всього за 10 місяців бойових дій підрозділом було складене, віддруковане та розіслане у війська більше 80 тисяч кодових книг. Після цього на обкладинці кодової книги «Колорадо» – останньої з серії «Річкових кодів» – було надруковано: «Запам'ятай цю групу: *DAM* – Код втрачений».

Крім того, під час Першої світової війни для шифрування повідомлень під час бойових дій армія США використовувала також і мову індійців. Так, у вересні 1918 року у скла-

ді 30-ї Піхотної дивізії, що діяла в координації з британськими військами і під британським командуванням, знаходилося декілька загонів індійців-зв'язківців «черокі», які брали участь у Другій битві на річці Сомме. У жовтні 14 індійців-зв'язківців «чокто» у складі 36-ї Піхотної дивізії допомогли експедиційним військам США виграти ряд боїв у ході Мюсаргонської кампанії у Франції. Протягом доби після того, як мова «чокто» почала використовуватися в бойових умовах, у діях відбувся поворот не на користь німців, а менш ніж через 3 доби війська Союзників вже переслідували відступаючі німецькі війська.

Характерною ознакою Першої світової війни, крім застосування воюючими сторонами нових видів озброєння – літаків, танків, підводних човнів, стала поява нового виду військової розвідки -радіорозвідки. її успіху і широкому розвитку сприяли інтенсивне застосування засобів радіозв'язку, численні порушення радистами правил радіообміну, передача по радіо секретних розпоряджень і наказів, зашифрованих з використанням нескладних код і шифрів. Разом з російською, англійською, французькою, німецькою і австро-угорською арміями радіорозвідка в роки Першої світової війни велася і підрозділами експедиційного з'єднання американських військ.

Пости підслуховування, до складу яких входили підготовлені військовослужбовці, які володіли німецькою мовою, розміщувалися в безпосередній близькості від районів

розташування німецьких військ. Підключивши телефонні апарати до дротових ліній зв'язку супротивника, вони здійснювали прослуховування та запис телеграфних і телефонних повідомлень, що передавались по них. Пости радіоперехоплення, розташовані, як правило, на значному видаленні від лінії фронту, дозволяли без безпосереднього зіткнення зі супротивником здобувати цінні відомості про його угрупування, дії та наміри. Можливості американської радіорозвідки істотно підвищувалися завдяки використанню постів радіопеленгації, що визначали місця розташування військових радіостанцій супротивника.

Конец ознакомительного фрагмента.