Peter Wright, Paul Greengrass, „Łowca szpiegów", Autobiografia oficera brytyjskiego kontrwywiadu. Pezłożyli: Witold Kalinowski i Eugeniusz Możejko.
Wydawnictwo OFFICINA, Warszawa 1991

Rozdział 13, str 164

Wielka operacja łamania szyfrów pod kryptonimem VENONA.

W latach 30-tych służby wywiadowcze, zarówno rosyjskie jak brytyjskie, zaczęły masowo stosować system jednorazowych kart kodowych. Jest to najbezpieczniejsza forma szyfrowania, ponieważ tylko nadawca i odbiorca dysponują analogicznymi kartami, składającymi się z liczb losowych. Jeśli każda taka para kart używana jest tylko raz, po czym niszczona, podsłuchujący przeciwnik nie ma żadnego dostępu do treści komunikatów. Chcąc zaszyfrować tym sposobem tekst, nadawca tłumaczy najpierw każde słowo na grupę cyfr, posługując się w tym celu stałą książką kodową. Powiedzmy, że pierwsze słowo komunikatu brzmi: „obrona", a w książce kodowej odpowiada mu grupa: 3765. Do liczby 3765 dodaje nadawca pierwszą grupę cyfr z jednorazowej karty, dajmy na to: 1196, stosując system Fibonacciego, otrzymuje w sumie grupę: 4851 - i tę wysyła w eter. Odbiorca postępuje w odwrotnej kolejności: odejmuje, tym samym sposobem.pierwszą liczbę z jednorazowej karty od pierwszej liczby przekazu radiowego i dopiero dla obliczonej różnicy znajduje odpowiednik w książce kodowej. (Jest to więc, w istocie, szyfrowanie dwustopniowe).

Jeśli w akcji VENONA udało się złamać tego rodzaju szyfr, to tylko dlatego, że Rosjanie zlekzeważyli jego kardynalną zasadę: ponieważ w pierwszych latach wojny mieli za mało oryginalnych tablic liczb losowych, a potrzeby ich systemów łączności były olbrzymie, zdecydowali się więc powtórzyć te same zestawy kart (bloczki szyfrowe) i rozsyłać je do różnych placówek na Zachodzie. W gruncie rzeczy ryzyko zdemaskowania w ten sposób niektórych przekazów było znikome. Rosjanie wysyłali w świat ogromne ilości komunikatów na różnych kanałach: dla ambasadorów, dla GRU, dla floty, dla KGB; był też oddzielny kanał łączności handlowej, obsługujący wielkie dostawy sprzętu wojennego z Zachodu na front wschodni. Ten kanał skupiał około 80% tajnych transmisji sowieckich. Dwa takie same bloczki mogły trafić, np. do rezydenta KGB w ambasadzie w Waszyngtonie i do sowieckiego radcy handlowego w Meksyku.

Tuż po zakończeniu wojny znakomity amerykański kryptoanalityk Meredith Gardner, z Agencji Bezpieczeństwa Sił Zbrojnych (poprzednik NSA), rozpoczął prace nad zwęglonymi szczątkami sowieckiej książki kodowej, znalezionymi na pobojowisku w Finlandii. Choć niekompletna, książka zawierała jednak niektóre grupy cyfr, odpowiadające najczęstszym instrukcjom w tajnych przekazach radiowych, takim np. jak „Spell" i „Endspell" („literuję" i „koniec literowania"). Występują one często, ponieważ każda książka kodowa ma tylko ograniczoną liczbę haseł; kiedy nadawca chce przekazać słowo, dla którego w książce nie ma odpowiednika cyfrowego - dotyczy to np. wszystkich nazw i nazwisk - musi je przeliterować, co zapowiada hasłem „Spell" i kończy hasłem „Endspell", by nie wprowadzać w błąd odbiorcy.

Znając te najczęściej występujące grupy cyfr Gardner zanalizował dużo rosyjskich przekazów radiowych - i stwierdził, że w wielu emisjach, przekazywanych w różnych „kanałach", zdarzają się dokładne powtórzenia, z czego wynikało, że Rosjanie zastosowali dwukrotnie te same bloczki jednorazowych kart. Po pewnym czasie udało się mu zidentyfikować kilka

„bliźniaczych par” (dwie linie łączności korzystające z tych samych bloczków) - i podjął próbę złamania tych szyfrów. Początkowo nikt nie wierzył w taką możliwość; wysiłki Gardnera wzięto na serio dopiero wtedy, kiedy zdołał odczytać fragment depeszy rosyjskiego ambasadora w Waszyngtonie - do Moskwy. Odczytał mianowicie angielskie zdanie: „Defense does not win wars” („Obroną nie wygrywa się wojen”), zawarte w sekwencji Spell - Endspell. Był to, ponad wszelką wątpliwość, tytuł świeżo wydanej w USA książki o strategii obronnej.

Identyfikacja „bliźniaków” nie gwarantowała jeszcze możliwości odczytania komunikatów. Książka kodowa była zrekonstruowana tylko w skromnej części, analitycy musieli więc posługiwać się dodatkowymi informacjami. Jeśli np. stwierdzili tożsamość bloczków szyfrowych linii KGB Waszyngton - Moskwa i linii handlowej Nowy Jork - Moskwa, mogli zdobywać dodatkowe informacje o tej ostatniej z manifestów okrętowych, listów przewozowych, rozkładów rejsów, kalendarza przypływów i odpływów, itd. Te informacje, e zestawieniu z materiałem cyfrowym komunikatów, pozwalały analitykom odgadywać, co oznaczają poszczególne grupy cyfr w tajnych komunikatach handlowych. Odczytanie komunikatu na jednej z „bliźniaczych” linii powiększało znaną nam część książki kodowej i otwierało drogę do tajników drugiej linii.

Brytyjczycy i Amerykanie opracowali skuteczne metody robocze dla VENONY. Podstawowa nosiła nazwę: „indeks okna”. Ilekroć rozszyfrowano nowe słowo lub sformułowanie, sporządzano wykaz wszystkich kontekstów, w jakich występowało ono w „bliźniaczych” przekazach. Ściślej: rejestrowano wszystkie nie rozszyfrowane jeszcze grupy cyfr bezpośrednio sąsiadujących w tych przekazach ze znanym już „oknem”. Z reguły po dłuższej obserwacji w takim „indeksie okna” pojawiały się powtórzenia tych samych liczb. Analiza tych powtórzeń dawała często wystarczającą informację dodatkową, by rozszyfrować powtarzającą się grupę cyfr i „rozszerzyć okno”. Inną stosowaną metodą było „przeciąganie”. Kiedy pojawiła się sekwencja Spell - Endspell, w której nasi kryptoanalitycy rozpoznawali tylko niektóre litery, badano przy użyciu maszyn liczących wszystkie zarejetrowane przekazy danej linii, a także linii „bliźniaczej”, szukając powtórek nieznanych jeszcze grup we wszystkich takich sekwencjach. Kontekst tych powtórek pozwalał w końcu zidentyfikować zaszyfrowaną w danej liczbie literę.

Była to niesłychanie żmudna praca; często wiedza naszych analityków posuwała się zaledwie o parę słów miesięcznie; czasem jednak robiła gwałtowne postępy - kiedyś Amerykanie odczytali za jednym zamachem cały długi tekst z linii ambasadoeskiej. Często pojawiały się niespodziewane utrudnienia; zdarzało się, że Rosjanie używali jednorazowych kart w sposób niekonwencjonalny, czytając je, np. na przemian od góry i od dołu albo w innym wymyślonym ad hoc porządku. Bardzo utrudniało to zwłaszcza wstępną fazę operacji VENONA, tzn. identyfikację „par bliźniaczych”. Były też kłopoty z książkami kodowymi; czasem Rosjanie po prostu zmieniali je; poza tym, o ile linie ambasadorskie, handlowe i GRU używały książek ułożonych alfabetycznie, jak zwykły słownik - dzięki czemu analitycy mogli z cech grupy cyfr domyślić się od razu pod jaką literą i na której stronie należy jej szukać - to KGB używało specjalnej wielotomowej książki, w której hasła były rozrzucone przypadkowo, co sprawiało analitykom wątpliwą „rozkosz łamania głowy”.

TEKST PRZEKAZU

TWÓJ KOMUNIKAT Z 74689 I 02985 47111 67789 88005 62971 DOTYCZĄCY LITERUJĘ HICKS KONIECLIT 55557 81045 10835 68971 71129 SKRAJNĄ OSTROŻNOŚĆ W CHWILA OBECNA 56690 12748 92640 00471 LITERUJĘ STANLEY KONIECLIT 37106 72885 MIESIĘCZNIE DO NASTĘPNA INSTRUKCJA

PODPIS PRZEKAZU

Gardner uważał, nie bez racji, że wymyślona przezeń metoda łamania szyfró była arcydziełem czystej matematyki - i mierził go zrobiony z niej użytek.

Cipher Systems, H.Beker & Fred Piper, str 148 - 149

There is one particular system which offers perfect secrecy and which deserves special mention, the one - time pad. In this system there is an upper bound, N say, on the length of all possible messages, and the numbers of keys, which are all equally likely, is at least as large as N. If the message to be enciphered is $m_1m_2m_3 ... m_n$ then a random sequence $k_1k_2k_3 ... k_n$ is selected (By this we mean that each k_i is chosen independently of any other