УДК 681.188

ПРОБЛЕМИ КРИПТОЗАХИСТУ ШИФРУВАЛЬНОЇ МАШИНКИ «ЕНІГМА»

Бабяк Євгенія Олексіївна, Масальська Олена Олександрівна
Державний ВНЗ «Національний гірничий університет», м. Дніпропетровськ, Україна,
http://bit.nmu.org.ua, E-mail: burnbeforeyou@yahoo.com

Шифрувальні пристрої дозволяють захистити інформацію, передану по радіоканалу, від перегляду сторонніми особами, і насамперед, спецслужбою супротивника. У загальному випадку букви і цифри повідомлення замінюються іншими символами, роблячи його абсолютно незрозумілим. Найпростіші шифри, що застосовувалися протягом століть, використовували схему прямого заміщення однієї букви інший, причому щоразу однієї і тієї ж.

Ключові слова – криптозахист; надійність шифру; безпека конфіденційної інформації .

ВСТУП

Нові способи шифрування представлялися настільки надійними, що, здавалося, противнику не вдасться їх розгадати. Тим не менш, багато з застосовувалися тоді шифрів були розкриті вже під час другої світової війни завдяки таланту вчених-криптографов і застосуванню електронно-обчислювальних машин.

«Опинитися в потрібному місці в потрібний час» - саме цим девізом я можна охарактеризувати успішність криптомашини Енігма, яку німецьке командування вважало одним з найнадійніших шифрувальних пристроїв. У 1917 році голландець Кох запатентував електричний роторний шифрувальний пристрій для захисту комерційної інформації. У 1918 році німець Шербіус купив цей патент, доопрацював його і побудував шифрувальну машину Енігма (від грец. Ανιγμα - «загадка»). Сам пристрій працював на поліалфавітному шифрі підстановки. Простою версією поліалфавітних шифрів є шифр Віженера [3]. Для свого часу це був досить просунутий метод, адже не знаючи ключового слова, його дуже важко було зламати. Чотирьохроторну машину можна було налаштувати на будь-який спосіб кодування, а способів таких було - $2 \cdot 10^{145}$. І кожен по-різному шифрував текст [1].

ОСНОВНИЙ ПРИНЦИП РОБОТИ

Ротори - серце Енігми. Кожен ротор представляв собою диск приблизно 10 см в діаметрі, зроблений з ебоніту або бакеліта, з пружинними штирьовими контактами на одній стороні ротора, розташованими по окружності. На іншій стороні знаходилося відповідну кількість плоских електричних контактів. Штирові і плоскі контакти відповідали буквах в алфавіті (зазвичай це були 26 букв від A до Z). При зіткненні контакти сусідніх роторів замикали електричний ланцюг. Всередині ротора кожен штирьовий контакт був з'єднаний з одним із плоских. Порядок з'єднання міг бути різним. При використанні декількох роторів у зв'язці (зазвичай трьох або чотирьох) за рахунок їх постійного руху виходив більш надійний шифр [1].

ОСОБЛИВОСТІ ТА ПЕРЕВАГИ ПРИСТРОЮ

«Енігма» була розроблена таким чином, щоб безпека зберігалася навіть у тих випадках, коли шпигунові відомі роторні схеми, хоча на практиці налаштування зберігаються в секреті. Більшість ключів зберігалися лише певний період часу, зазвичай добу. Однак для кожного нового повідомлення задавалися нові початкові позиції роторів. Це обумовлювалося тим, що якщо число повідомлень, посланих з ідентичними налаштуваннями, буде велике, то криптоаналитик, який досконало вивчив стільки повідомлень, може підібрати ключ до повідомлень, використовуючи частотний аналіз. Для надійності шифру так само часто вживані слова та імена дуже сильно варіювалися. Наприклад, слово «Minensuchboot» могло бути написано як «MINENSUCHBOOT», «MINBOOT», «MMMBOOT» або «MMM354». Щоб ускладнити криптоаналіз, окремі повідомлення не містили понад 250 символів. Довші повідомлення розбивалися на частини, кожна з яких використовувала свій ключ.

СИСТЕМИ ЗНЕШКОДЖЕННЯ «ЗАГАДКИ» ПІД КОДОВОЮ НАЗВОЮ «ULTRA»

Злом англійцями німецьких шифрувальних машин, тобто машинне розгадування способу шифрування текстів в них, отримала англійську назву ULTRA. Немашинні методи дешифрування були занадто трудомісткими і в умовах війни неприйнятними. Для цієї роботи англійці об'єднали приблизно 10 000 осіб, у тому числі математиків, інженерів, лінгвістів, перекладачів, військових експертів, а також інших співробітників для сортування даних, їх перевірки та архівування, для обслуговування машин. Це об'єднання носило назву BP (Bletchley Park - Блетчлі парк), воно знаходилось під контролем особисто Черчілля. Отримана інформація виявилася в руках союзників могутньою зброєю. Англійські військові і особисто Черчиль вимагали постійної уваги до розшифровки повідомлень. Починаючи з літа 1940р. англійці розшифровували всі повідомлення, зашифровані за допомогою Енігми. Тим не менш, англійські фахівці безперервно займалися вдосконаленням дешифровальной техніки. До кінця війни англійські дешифратори мали на своєму озброєнні 211 цілодобово працюючих дешифрирувальних пристроїв. Їх обслуговували 265 механіків, а для чергування були залучені 1675 жінок. Роботу творців цих машин оцінили через багато років,

коли спробували відтворити одну з них: через відсутність на той момент необхідних кадрів, робота з відтворення відомого пристрою тривала кілька років і залишилася незакінченою!

Створена тоді Т'юрінгом інструкція по створенню дешифрируются пристроїв перебувала під забороною до 1996 року. Серед засобів дешифрування був метод «примусовою» інформації: наприклад, англійські літаки руйнували пристань у порту Калле, свідомо знаючи, що далі слідуватиме повідомлення німецьких служб про це з набором заздалегідь відомих англійцям слів! Крім того, німецькі служби передавали це повідомлення багато разів, щоразу кодуючи його різними шифрами, але слово в слово.

Нарешті, найважливішим фронтом для Англії була підводна війна, де німці використовували нову модифікацію ЕнігмаМ3. Англійський флот зміг вилучити таку машину з захопленого ними німецького підводного човна. З 1 лютого 1942 ВМФ Німеччини перейшов на користування моделлю М4. Але деякі німецькі повідомлення, зашифровані по-старому, помилково містили інформацію про особливості конструкції цієї нової машини. Це сильно полегшило завдання команді Т'юрінга. Уже в грудні 1942р. була зламана Енігма М4. 13 грудня 1942 англійське Адміралтейство отримало точні дані про місцезнаходження 12 німецьких підводних човнів в Атлантиці.

На думку Т'юрінга, для прискорення дешифрування необхідно було переходити до використання електроніки. 7 листопада 1942 Тюрінг відправився в США, де разом з командою з лабораторій Белла були вдосконалені американські дешифрувальні машини, так що Енігма М4 була зламана остаточно і до кінця війни давала англійцям і американцям вичерпну розвідувальну інформацію. Тільки в листопаді 1944 року у німецького командування виникли сумніви в надійності своєї шифрувальної техніки, проте ні до яких заходів це не призвело [4].

ВИСНОВКИ

Енігма представляла собою досить зручну шифрувальну машину: одержуваний шифр був досить складний, а сама процедура кодування розкодування була досить проста. Також невід'ємним перевагою шифру Енігми є висока швидкість кодування розкодування. Крім того, процедура кодування дуже проста з вигляду і наочна.

З появою комп'ютерів надійність такого шифру впала, тому код має досить багато важливих особливостей, що спрощують злом, тому в сучасних системах таке шифрування застосовують досить рідко.

СПИСОК ВИКОРИСТАННОЇ ЛИТЕРАТУРИ

1. Жельников В. Криптографія від папірусу до комп'ютера. М .: ABF, 1996. 336 с.
2. Смарт Н. Криптографія. Серія «Світ програмування». Пров. з англ. С. А. Кулешова / Под ред. С. К. Ландо. М .: Техносфера, 2005. 528 с.
3. Шнайер Б. Прикладна криптографія. Протоколи, алгоритми, вихідні тексти на мові Сі. М .: Тріумф, 2003. 816 с.
4. Таємниця проекту Ultra // OSP.ru, 2003-07-08 Режим доступу: http://www.osp.ru/os/2003/07-08/183294/