Енігма

Олексій Лубинець, 5 курс, ФВЕ

Об'єктно-орієнтоване програмування

14 травня 2018 р.

Загальні відомості

- сімейство переносних електромеханічних роторних шифрувальних машин.

- використовується з 20-х років
- комерційне призначення
- військове призначення (зокрема у Німеччині)
- близько 100000 екземплярів

Історія

- 23 лютого 1918 року німецькому інженеру Артуру Шербіусу був виданий патент на шифрувальну машину
- 1923-1924 - “Енігма А” представлена на конгресі Всесвітнього поштового союзу
- 1925 Німецький Військово-морський флот почав використовувати “Енігму”
- 15 липня 1928 німецька Армія впровадила власну модель “Енігми”
- 1932 - шифр “Енігми” вперше був розкритий польськими спеціалістами

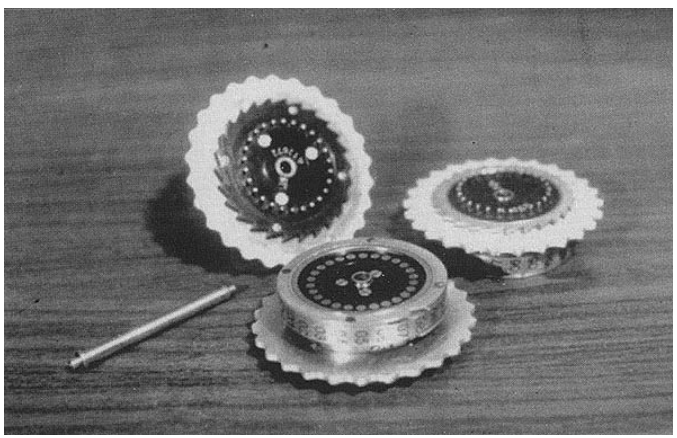
Принцип дії

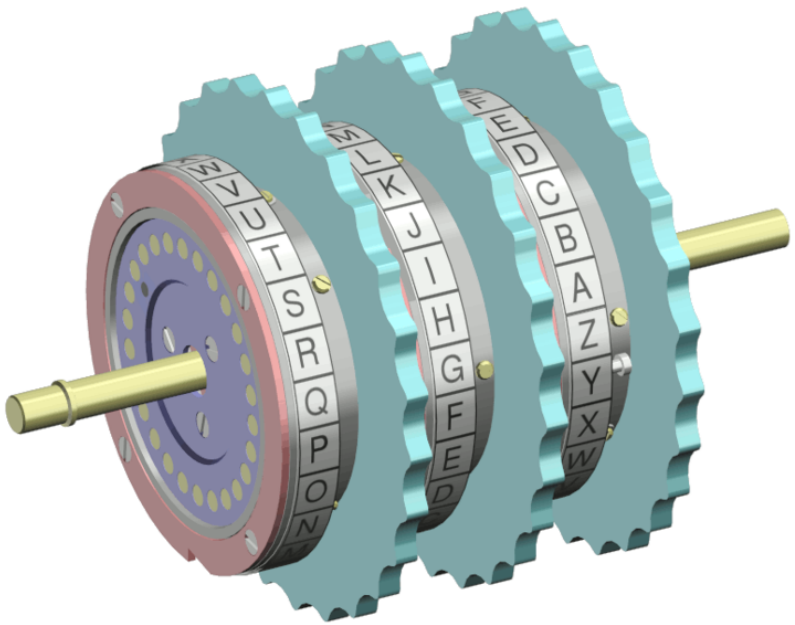
Конкретний механізм роботи міг бути різним, але загальний принцип був такий: при кожному натисканні на клавішу найправіший ротор зсувається на одну позицію, а при певних умовах зсуваються і інші ротори. Рух роторів призводить до різних криптографічних перетворень при кожному наступному натисканні на клавішу на клавіатурі.

Ротори - серце "Енігми". Кожен ротор являв собою диск приблизно 10 см в діаметрі, зроблений з ебоніту або бакеліту, з пружинними штирьовими контактами на правій стороні ротора, розташованими по колу.

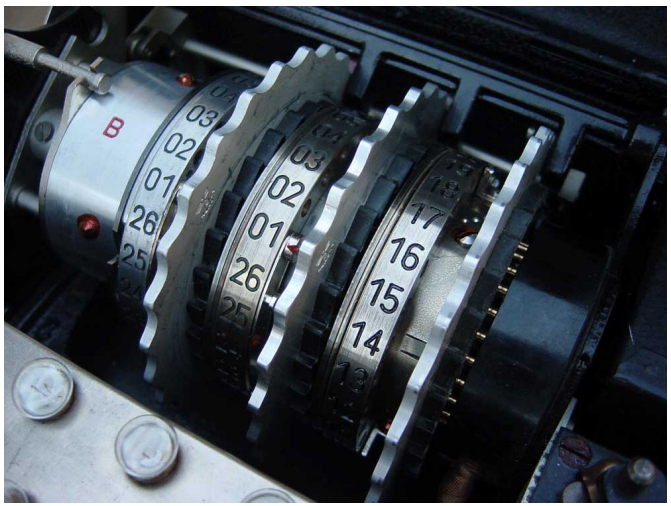
Сам по собі ротор здійснював дуже простий тип шифрування: елементарний **шифр заміни**. Наприклад, контакт, який відповідає за букву E, міг бути з'єднаний з контактом літери T на іншій стороні ротора. Але при використанні декількох роторів в зв'язці (зазвичай трьох або чотирьох) за рахунок їх постійного руху виходить більш надійний шифр.

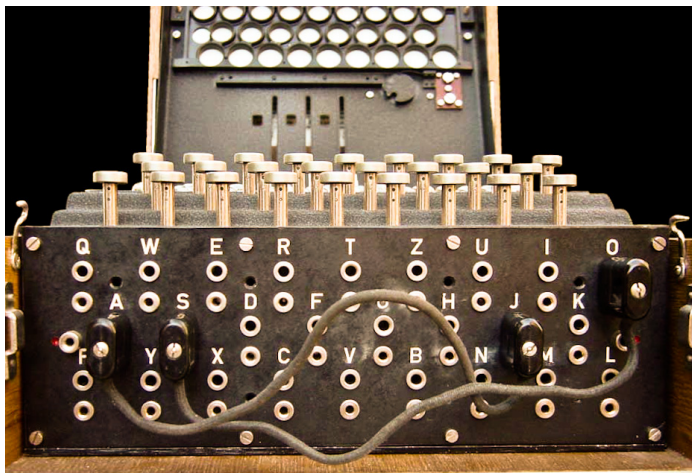
Ротори





Ротори та комутаційна панель





Комутаційна панель внесла величезний внесок в ускладнення шифрування машини, навіть більший, ніж введення додаткового ротора. З “ Енігмою ” без комутаційної панелі можна впоратися практично вручну, однак після додавання комутаційної панелі зломщики були змушені конструювати спеціальні машини.

Процедура використання

Щоб повідомлення було правильно зашифроване й розшифровано, машини відправника і одержувача повинні були бути однаково налаштовані, конкретно ідентичними повинні були бути: вибір роторів, початкові позиції роторів і з'єднання комутаційної панелі.
Більшість ключів зберігалася лише певний період часу, зазвичай добу. Однак для кожного нового повідомлення задавалися нові початкові позиції роторів. Це зумовлювалося тим, що якщо число повідомлень, які були надіслані з ідентичними налаштуваннями, буде велике, то криптоаналитик, досконально вивчив кілька повідомлень, може підібрати шифр до повідомлень, використовуючи **частотний аналіз**.

Абревіатури та директиви

- пробіл пропускався або замінювався на “ X ”
- кома - на ZZ
- знак питання - на FRAGE або FRAQ
- комбінація CH - на Q
- два, три або чотири нулі замінялися словами «CENTA», «MILLE» і «MYRIA» відповідно

Часто вживані слова та імена дуже сильно варіювалися. Наприклад, слово «Minensuchboot» (мінний тральщик) могло бути написано як «MINENSUCHBOOT», «MINBOOT», «MMMBOOT» або «MMM354».
Щоб ускладнити криптоаналіз, окремі повідомлення не містили понад 250 символів. Довші повідомлення розбивалися на частини, і кожна частина використовувала свій ключ. Крім того, іноді оператори спеціально забивали зашифровані повідомлення «сміттям» (наприклад, нескладний набір букв, не пов’язані з основним текстом слова), для ускладнення дешифрування перехоплень противником.

Криптоаналіз "Енігми"

Протягом всього періоду активного застосування «Енігма», різні урядові організації країн Європи робили спроби «злому» машини з метою захисту від наростаючої загрози з боку Німеччини. «Енігма» була необхідна Німеччини для проведення швидкого і скоординованого наступу проти ряду країн в рамках Другої світової війни. У довоєнний період найбільших успіхів в дешифрування повідомлень «Енігми» досягло польське Бюро шифрів і особисто Маріан Реевскій. Під час Другої світової війни пальму першості в справі криптоанализа «Енігми» взяв центр британської розвідки «Station X», також відомий як Блетчлі-парк.

- атака на основі підібраного відкритого тексту
- демонстративне мінування
- Enigma@home