РОЗДІЛ 2. Теорія чисел і криптографія

Тема 7. Класична криптографія (закінчення)

План лекції

- **Класична криптографія. Шифри заміни**
  - **Шифри зсуву і афінні шифри**
  - **Криптоаналіз**
  - **Поліалфавітні шифри**
  - **Що таке криптосистема?**
- **Історична довідка**

ШИФРИ ЗАМІНИ

Шифри зсуву і афінні шифри

Одним із найбільш ранніх відомих користувачів криптографії був давньоримський імператор Юлій Цезар. Він зашифровував свої повідомлення у спосіб, коли кожна буква заміщується деякою іншою, а саме тою, що знаходиться в алфавіті через три позиції. Стосовно української абетки це означає, що А міняється на Г, Б на Ґ, В на Д, Г на Е і т.д. Останні ж три букви абетки Ь, Ю та Я заміщуються буквами, що знаходяться через три позиції *циклічно*, тобто переходять у А, Б та В, відповідно. Щоб описати цей *шифр Цезаря* математично, спочатку замінимо кожну букву українського алфавіту елементом множини z_{33}, тобто цілим числом від 0 до 32: кожна буква замінюється своїм порядковим номером, причому нумерація починається з 0. Наприклад, А міняється на 0, Ї – на 12, Я – на 32.

Метод шифрування Цезаря можна подати функцією f, яка визначена на множині $\mathbf{z}_{33}$ і набуває значення із цієї ж множини:

$$f(p)=(p+3)\,\mathbf{mod}\,33.$$

Під час шифрування повідомлення буква, яка представлена p міняється на букву, представлену $(p+3)\bmod 33$.

Приклад. Зашифруємо шифром Цезаря повідомлення «Я ПРИЇДУ ЗАВТРА». Спочатку замінимо кожну букву її номером, тоді одержимо:

32 19 20 10 12 5 23 9 0 2 22 20 0.

Тепер замінимо кожний із цих номерів p на $(p+3)\,\mathbf{mod}\,33$, це дасть:

2 22 23 13 15 8 26 12 3 5 25 23 3.

Повертаючись тепер від цифр назад до букв, одержимо зашифроване повідомлення:

«В ТУЙЛЖЦ ЇГДХУГ».

Для одержання оригінального повідомлення із секретного, зашифрованого шифром Цезаря, використовують функцію f^{-1}, обернену до f. Ця функція відображає ціле число p із множини Z_{33} у $f^{-1}(p)=(p-3)\,\mathbf{mod}\,33$. Процес знаходження оригінального повідомлення із зашифрованого називають *дешифруванням*.

Зауваження. У разі шифрування повідомлень, написаних англійською мовою, очевидно використовують функцію $f(p)=(p+3)\,\mathbf{mod}\,26$, а для розшифрування – функцію $f^{-1}(p)=(p-3)\,\mathbf{mod}\,26$. Область визначення та область значень обох функцій – множина Z_{26}.

Шифр Цезаря можна узагальнити в різний спосіб. Наприклад, замість зсуву числового еквівалента кожної букви на 3, можна зсувати числовий еквівалент кожної букви на k, отже

$$f(p)=(p+k)\ \mathbf{mod}\ 33.$$

Такий шифр називають *шифром зсуву*. Зазначимо, що для розшифрування тут має бути використана функція $f^{-1}(p)=(p-k)\ \mathbf{mod}\ 33$. Тут ціле число k називають *ключем*.

Подальше узагальнення шифру зсуву, яке трохи посилює його стійкість до розкриття, є використання функції $f(p)=(ap+b)\ \mathbf{mod}\ 33$, де a та b цілі, які вибирають так, щоб функція f була **бієкцією**. (Для того, щоб функція $f(p)=(ap+b)\ \mathbf{mod}\ 33$ була бієкцією, необхідно й достатньо, щоб $\gcd(a,33)=1$). Таке відображення називають *афінним перетворенням*, а відповідний шифр – *афінним шифром*.

Приклад. Якою буквою буде замінена буква Ю, якщо для шифрування використати функцію $f(p)=(7p+3)\ \mathbf{mod}\ 33$? Оскільки 31 репрезентує букву Ю, то використовуючи задану шифрувальну функцію, дістанемо $f(31)=(7\cdot 31+3)\ \mathbf{mod}\ 33=22$. Оскільки 22 репрезентує букву Т, то в зашифрованому повідомленні Ю заміниться на Т.

Тепер покажемо, як розшифрувати повідомлення, яке зашифроване афінним шифром. Припустімо, що $c = (ap + b) \bmod 33$, причому $\gcd(a, 33) = 1$. Для дешифрування нам потрібно показати, як виразити p через c. Щоб це зробити, розглянемо шифрувальну конгруенцію $c \equiv ap + b \pmod{33}$ і розв'яжемо її відносно p. Щоб це зробити, спочатку віднімемо b від обох частин конгруенції, тоді матимемо $c - b \equiv ap \pmod{33}$. Тому що $\gcd(a, 33) = 1$, існує обернене a^{-1} до a за модулем 33. Помножимо обидві частини останньої конгруенції на a^{-1}, тоді одержимо $a^{-1}(c - b) \equiv a^{-1}ap \pmod{33}$. Оскільки $a^{-1}a \equiv 1 \pmod{33}$, то $p \equiv a^{-1}(c - b) \bmod 33$. Це визначає p, бо p належить Z_{33}.

Криптоаналіз

Процес відновлення закодованого тексту з шифротексту без знань як методу шифрування, так і ключа відомий як *кританаліз* або *злам коду*. Загалом, криптоаналіз – важкий процес, особливо коли метод шифрування невідомий. Ми не будемо обговорювати криптоаналіз в цілому, але пояснимо, як зламати повідомлення, зашифровані за допомогою шифру зсуву. Якщо ми знаємо, що зашифроване повідомлення створювалося шляхом шифрування за допомогою шифру зсуву, ми можемо спробувати відновити повідомлення, перемістивши всі символи шифротексту на кожну з 26 можливих змін (для англійського алфавіту). Одне з них гарантовано є текстом повідомлення. Однак ми можемо використовувати більш розумний підхід, на якому можна побудувати криптоаналіз шифротексту, отриманого також і за допомогою інших шифрів. Основний інструмент для криптоаналізу шифротексту, зашифрованого за допомогою шифру зсуву, – це підрахунок частоти літер у шифротексті. Ось дев'ять найпоширеніших букв англійського тексту та їх приблизні відносні частоти: E 13%, T 9%, A 8%, O 8%, I 7%, N 7%, S 7%, H 6% і R 6%. Спочатку знаходимо відносні частоти літер у шифротексті. Розглядаємо найпоширеніші букви в шифротексті в порядку частоти. Природно вважати, що найбільш поширена літера в шифротексті отримується за допомогою шифрування E. Тоді визначаємо значення зсуву за цією гіпотезою, скажімо, k. Якщо повідомлення, отримане зміщенням шифротексту на $-k$, має сенс, вважаємо, що наша гіпотеза правильна і що ми маємо правильне значення k. Якщо це не має сенсу, далі припускаємо, що найбільш поширена літера в шифротексті отримується за допомогою шифрування T, другої за поширеністю літери англійської мови; знаходимо k за цим припущенням, зсуваємо літери повідомлення на $-k$ і дивимося, чи отримане повідомлення має сенс.

Якщо цього не відбувається, ми продовжуємо цей процес. Аналогічну методику можна використати й для української абетки. Наведемо відносні частоти найпоширеніших букв української мови: О 8,2%, Н 7%, А 7%, И 5,6%, Т 5,1%, В 4,6%, Е 4,3%, Р 3,8%, І 3,7% та С 3,6%.

Приклад. Припустимо, що ми перехопили шифр-повідомлення ZNK KGXRE HOXJ MKZY ZNK CUXS, і знаємо, що був застосований шифр зсуву. Яким було оригінальне повідомлення?

Перехоплене повідомлення було зашифровано за допомогою шифру зсуву, тому починаємо з обчислення частоти букв у шифротексті. Найпоширеніша літера у наведеному шифротексті – це K. Отже, ми припускаємо, що шифр зсуву замінив літеру E на літеру K. Якщо ця гіпотеза правильна, то $10 = 4 + k \bmod 26$, тому $k = 6$. Далі зсуваємо літери повідомлення на −6, отримуючи THE EARLY BIRD GETS THE WORM. Оскільки це повідомлення має сенс, то гіпотеза, що $k = 6$, правильна.

Криптологія охоплює криптографію і криптоаналіз

Якщо повернутися до шифрів перестановки, які ми розглянули на попередній лекції, то з точки зору криптоаналізу їх важливою особливістю є те, що частоти, з якими букви зустрічаються у відкритому тексті та криптотексті співпадають, бо вони є інваріантними по відношенню до будь-якої перестановки.

Інша важлива особливість полягає в обмеженості розміру ключа. Це вимагає багаторазового використання ключа, що при за шифруванні довгих текстів полегшує криптоаналітичне дешифрування повідомлень. Тому перестановки доцільно використовувати у поєднанні із замінами у композиційних шифрах.

Можна довести, що шифр перестановки з періодом (довжиною ключа) l має $l!$ різних ключів. Якщо l є невеликим порівняно з довжиною тексту, то шифр перестановки розкривається спеціальним способом організованим аналізом частот біграм. Як саме це відбувається пояснимо на такому прикладі.

Нехай маємо криптотекст

ІЦКАЗИВИМЯИЛКИНОЙРЕСРПІНЗМЕЛБОПИРПИИТИНИИВІСВИТАЛП

і відомо, що він отриманий шифром перестановки з періодом 5. Розіб’ємо криптотекст на блоки по 5 букв і запишемо ці блоки один під одним, розташувавши текст у десяти рядках та п’яти стовпцях.

ІЦКАЗ		ЗАКЦІ
ИВИМЯ	← Криптотекст	ЯМИВИ
ИЛКИН	Відкритий текст →	НИКЛИ
ОЙРЕС		СЕРЙО
РПІНЗ		ЗНІПР
МЕЛБО		ОБЛЕМ
ПИРПИ		ИПРИП
ИТИНИ		ИНИТИ
ИВІСВ		ВСІВИ
ИТАЛП		ПЛАТИ
12345	← Номери стовпчиків →	54321

Зазначимо тепер, що дешифрування полягає у переставленні стовпчиків у належному порядку. Порядок цей, не знаючи ключа, можна знайти такими міркуваннями. На першій і третій позиціях другого рядка стоїть буква и. Це означає, що перший і третій стовпчики не можуть стояти поруч, бо тоді у відкритому тексті була б біграма ии, яка ніколи в українській мові не зустрічається, навіть коли з тексту вилучено пропуски між словами. Зауважимо також подвійні входження букви и у третьому і сьомому рядках і потрійне входження у восьмому рядку. Беручи до уваги позиції букви и у цих рядках, доходимо висновку, що не можуть бути поруч 1-й і 4-й, 2-й і 5-й стовпчики, а також будь-які два із 1-го, 3-го та 5-го стовпчиків.

Легко пересвідчитись, що ці вимоги задовольняють лише два розташування стовпчиків – (1, 2, 3, 4, 5) та (5, 4, 3, 2, 1). Оскільки перше розташування відповідає нашому криптотексту, то для розташування стовпчиків у відкритому тексті залишається єдина можливість – (5, 4, 3, 2, 1), що відповідає ключу $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 \end{pmatrix}$. Здійснивши обернену перестановку, прочитаємо розшифроване повідомлення по рядках:

З АКЦІЯМИ ВИНИКЛИ СЕРЙОЗНІ ПРОБЛЕМИ. ПРИПИНИТИ ВСІ ВИПЛАТИ.

У нашому криптоаналізі ми виходили з апріорно заданої інформації, що шифрування здійснювалось блоками довжини $l = 5$. Якби цього не було відомо, то подібний аналіз потрібно було б проводити для $l = 2, 3, \ldots$ аж допоки не було б досягнуто успіху. Для максимально наочної ілюстрації загального принципу приклад було підібрано так, що ключ визначався однозначно на підставі єдиного факту – біграма ии зустрічається в українській мові з нульовою частотою. У загальному випадку беруть до уваги й інші малоймовірні буквосполучення, і в результаті отримують систему обмежень на ключ, яка дає змогу суттєво скоротити перебір.

У сучасних електронних шифрах перестановки виконуються за допомогою елементів пам'яті у вигляді різних ліній затримки. У ручних шифрах, тобто шифрах «домашинної ери», шифри перестановки знаходили своє застосування.

Поліалфавітні шифри

Шифри зсуву та афінні шифри замінюють кожну букву алфавіту на іншу букву того ж алфавіту, незалежно від положення цієї букви у слові. Тому їх називають *моноалфавітними* шифрами. Розкриття таких шифрів успішно здійснюється аналізом частот появи букв у зашифрованому тексті. *Поліалфавітні* шифри можна потрактувати як такі шифри заміни, у яких позиція букви у відкритому тексті впливає на те, за яким саме правилом ця буква буде замінена. Розглянемо два класичні приклади.

1. *Шифр Віженера*. Відкритий текст і криптотекст записуються в одному й тому ж алфавіті.

Для букв x та y цього алфавіту означимо їхню суму $x + y$ як результат додавання номерів цих букв за модулем 26 для англомовного повідомлення і за модулем 33 – для україномовного. Нагадаємо що нумерація букв алфавіту починається з нуля. Наприклад, для української абетки маємо а + а = а, б + а = б, в + б = г, я + в = б. Цю операцію можна задати *таблицею Віженера* (див. у Додатку в кінці лекції).

Шифр Віженера застосовують до повідомлення, записаного в рядок без пропусків і розділових знаків. Ключем є слово в тому ж алфавіті. Якщо ключ коротший за повідомлення, то його записують багато разів поспіль, доки не вийде рядок такої ж довжини. *Саме тому шифр Віженера можна віднести до блокових шифрів.* Рядок із розмноженим ключем записують під рядком із повідомленням, і букви, що опинилися одна над одною, додають. Як результат отримують рядок тої ж довжини, який і є криптотекстом.

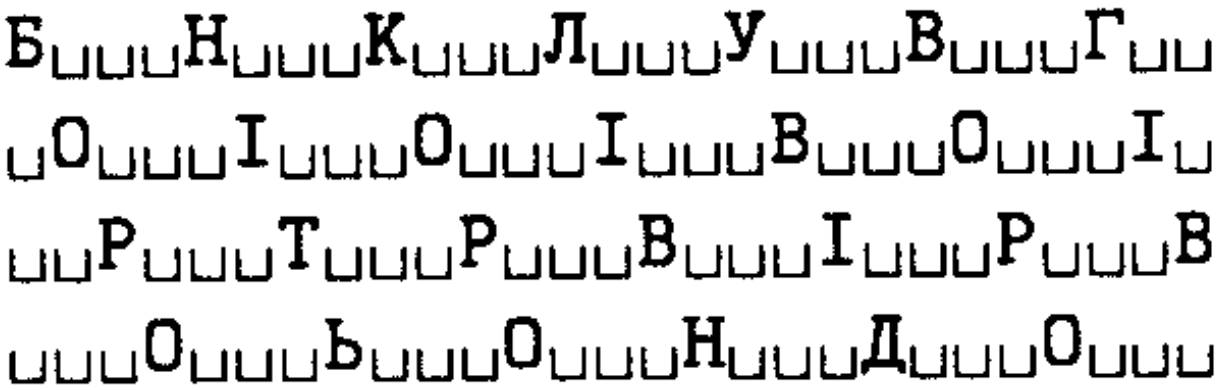
Для дешифрування потрібно від значень букв коду відняти значення букв ключа і результат щоразу редукувати за модулем 26 чи 33 залежно від алфавіту повідомлення.

Приклад. Шифрування наказу БОРОНІТЬ КОРОЛІВНУ ВІД ВОРОГІВ з ключем КЛЮЧ відбувається так

	Б	О	Р	О	Н	І	Т	Ь	К	О	Р	О	Л	І	В	Н	У	В	І	Д	В	О	Р	О	Г	І	В
+	К	Л	Ю	Ч	К	Л	Ю	Ч	К	Л	Ю	Ч	К	Л	Ю	Ч	К	Л	Ю	Ч	К	Л	Ю	Ч	К	Л	Ю		
	Л	А	О	Ї	Ю	Ц	Р	Ф	Ш	А	О	Ї	Щ	Ц	А	І	Ґ	Н	З	Я	М	А	О	Ї	Н	Ц	А		

Результатом шифрування є нижній рядок. Як можна побачити, при використанні шифру Віженера однаковим буквам у відкритому тексті можуть відповідати різні букви у криптотексті. Ця обставина, безперечно, ускладнює частотний криптоаналіз.

Шифр Віженера кілька століть уважався надійним, аж поки у 60 роках XIX століття офіцер прусського війська Касискі не виявив, що цей шифр все ж піддається частотному методу. Скористаємося попереднім прикладом, щоб пояснити головну ідею такого криптоаналізу. Шифр Віженера влаштований так, що при довжині ключа 4 кожна з чотирьох послідовностей відкритого тексту



перетворюється відповідно до деякого шифру зсуву (на 14, 15, 31 та 27 позицій відповідно – це для конкретного прикладу, що розглядається). За умови, що текст досить довгий, всі чотири довжини зсувів знаходяться стандартним підрахунком частот букв у відповідних послідовностях криптотексту.

Але як визначити із криптотексту, що застосовано ключ довжини саме 4? При уважному перегляді криптотексту зауважуємо в ньому однакові шматки: триграма (послідовність із трьох букв) аої зустрічається тричі, а біграма (послідовність із двох букв) ца – двічі. Природно припустити, що це зумовлено не випадковістю, а тим, що у відкритий текст у відповідних місцях входять одна й та сама триграма та біграма. У нашому випадку – це оро та ів. Те, що дві однакові поліграми відкритого тексту проявились у криптотексті, означає, що відстань між ними є кратною довжині ключа. (*Поліграма* – послідовність кількох букв тексту.) Відстані між різними входженнями триграми аої дорівнюють 8 і 12. Звідси висновок, що довжина ключа має ділити обидва ці числа, тобто дорівнює 1, або 2, або 4. Нам залишається випробувати лише ці три можливості, щоб знайти, яка з них у дійсності має місце.

Описана метода може розраховувати на успіх завжди, коли довжина тексту відносно до довжини ключа є великою. За цієї умови слід сподіватись, що текст міститиме чимало однакових біграм і триграм, і частині з них відповідатимуть однакові біграми та триграми в криптотексті з тої причини, що відстань між ними пропорційна до довжини ключа.

2. *Шифр з автоключем*. Цей шифр ґрунтується на ідеях Віженера і Кардано. Подібно до шифру Віженера, криптотекст отримують сумуванням відкритого тексту із послідовністю букв такої ж довжини. Але тепер цю послідовність формують хитріше – спершу записують ключ, а справа до нього дописують початковий відрізок самого відкритого криптотексту. Якщо розглянути той же приклад, то шифрування відбуватиметься так:

```
  БОРОНІТЬКОРОЛІВНУВІДВОРОГІВ
+ КЛЮЧБОРОНІТЬКОРОЛІВНУВІДВОР
-----------------------------
  ЛАОЇОЩЗЛЮЩЗЛЩЩТВДЙЙТХРЮУДЩТ
```

Важливо зазначити, що в наш час вживання в якості ключа для будь-якого шифру зручних для запам’ятовування ключових слів є досить ризикованим через *словникову атаку*. Найпростіший варіант цього методу криптоаналізу полягає в укладанні списку із, скажімо, 100000 найуживаніших ключових слів, включно із географічними назвами та екзотичними термінами. Рафінованіші версії включають лексику із вузькофахових публікацій автора повідомлення, послідовності із двох-трьох складів китайської мови тощо.

Що таке криптосистема?

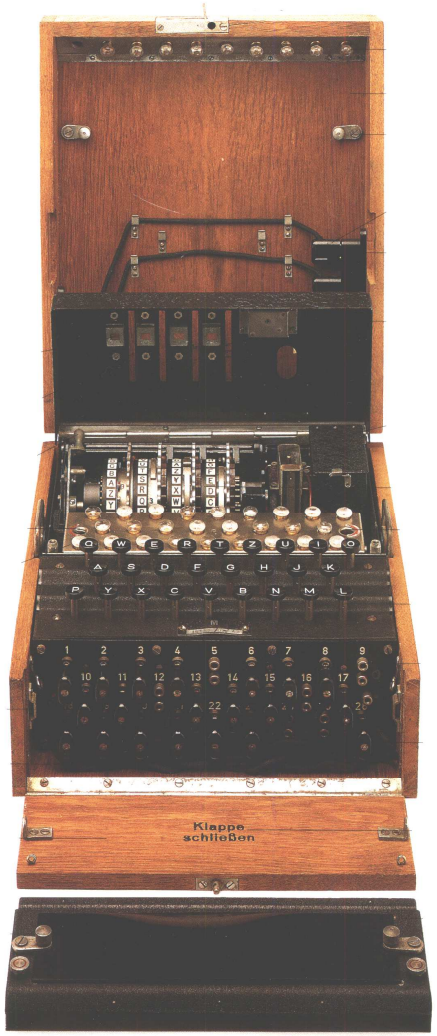
Ми визначили різні сімейства **шифрів заміни**: шифри зсуву, афінні шифри, шифр Віженера. Тепер ми введемо поняття криптосистеми, яке описує загальну структуру для визначення нових сімейств шифрів.

Криптосистема – це п'ятірка ($\mathcal{P}$, C, $\mathcal{K}$, $\mathcal{E}$, $\mathcal{D}$), де $\mathcal{P}$ – набір рядків відкритого тексту, C – набір рядків шифротексту, $\mathcal{K}$ – простір ключів (множина всіх можливих ключів), $\mathcal{E}$ – множина шифрувальних функцій і $\mathcal{D}$ – множина дешифрувальних функцій. Ми позначатимемо як E_k шифрувальну функцію із множини $\mathcal{E}$, що відповідає ключу k, і як D_k – дешифрувальну функцію із множини $\mathcal{D}$, яка дешифрує шифротекст, який був зашифрований за допомогою E_k, тобто $D_k(E_k(p)) = p$, для всіх рядків відкритого тексту p.

Тепер проілюструємо використання означення криптосистеми.

Приклад. Опишемо сімейство шифрів зсуву як криптосистему. Щоб зашифрувати рядок англійських букв шифром зсуву, спочатку переведемо кожну букву в ціле число від 0 до 25, тобто в елемент множини Z_{26}. Потім зсунемо кожне з цих цілих чисел за фіксованим модулем 26, і, нарешті, переведемо цілі числа знову до букв. Щоб застосувати визначення криптосистеми для шифру зсуву, ми припускаємо, що наші повідомлення вже є цілими числами, тобто елементами множини Z_{26}. Тобто ми припускаємо, що переклад між буквами і цілими числами знаходиться поза криптосистемою. Отже, і безліч рядків відкритого тексту $\mathcal{P}$, і безліч рядки шифротексту C – це множина рядків з елементів множини Z_{26}. Множина ключів $\mathcal{K}$ – це множина можливих зсувів, тому $\mathcal{K} = Z_{26}$. Множина $\mathcal{E}$ складається з функцій вигляду $E_k(p) = (p + k)$ **mod** 26, а множина $\mathcal{D}$ функцій дешифрування збігається з множиною функцій шифрування, де $D_k(p) = (p - k)$ **mod** 26.

ІСТОРИЧНА ДОВІДКА

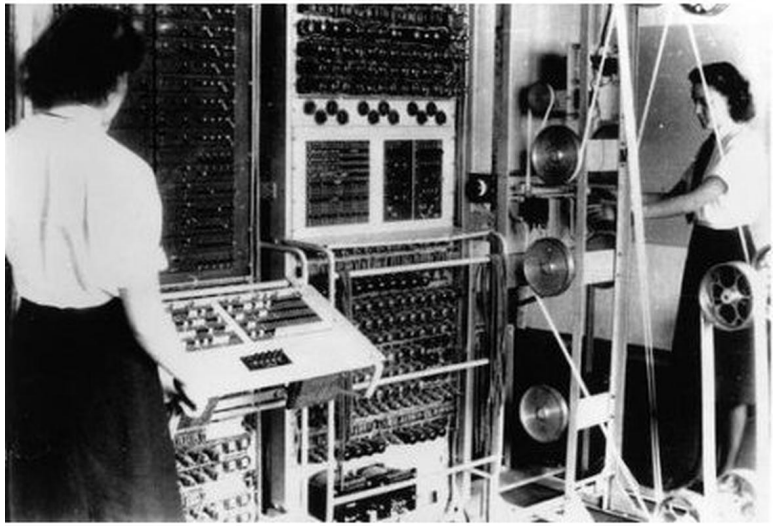


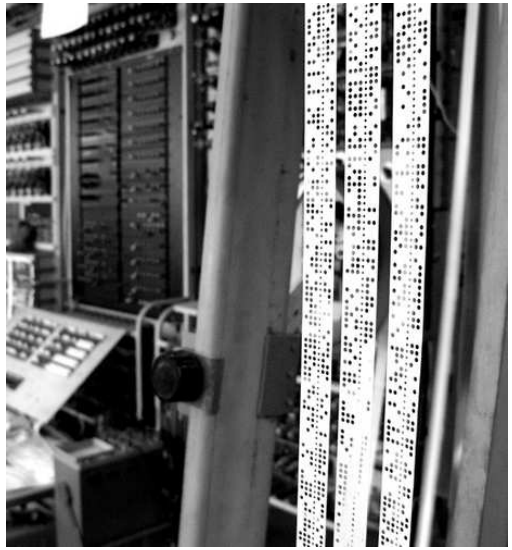
ENIGMA

У 20-х роках минулого століття були винайдені роторні шифрувальні пристрої, які вдосконалювались упродовж наступних десятиліть та інтенсивно використовувались під час ІІ світової війни. Прикладом може служити відомий німецький шифр *Enigma*. Роторні системи реалізовували багаторівневу композицію шифрів Віженера, що давало шифр з дуже великим періодом. Цей шифр було зламано в Англії (в Блетчлі-Парку) великою групою спеціалістів під керівництвом Алана Тьюрінга.

Здебільшого це були молоді талановиті люди, випускники або студенти Кембриджа і Оксфорда. Хоча пізніше, через зростання обсягу роботи, співробітників набирали навіть через оголошення, які подавалися як конкурси кросвордів. Після підписання акту секретності «переможців» відправляли в Блетчлі-Парк. Нестандартне мислення і творчий підхід в роботі, ексцентричність дешифрувальників – своєрідних хакерів (серед них Гордон Уелчмен, Джон Тілтмен і Алан Тьюрінг) – не змусили чекати результатів. Людей з аналітичними і математичними здібностями збирали звідусіль. Кожен день опівночі німецькі шифрувальні служби міняли коди, кількість комбінацій кодів Enigma досягала 150×10^{18}, тому невпинно проводився набір працівників в Блетчлі-Парк. Головними вимогами до співробітників були високі розумові здібності, висока працездатність і вміння мовчати.

Ситуація набирала обертів, було потрібно нове рішення, яке б дозволило обробляти інформацію за допомогою цифр, розшифровувати все автоматично. Справжній інтелектуальний і технічний прорив – обчислювальна машина **Colossus** (1942 рік). Всього було побудовано 10 Colossus; єдиний працюючий екземпляр зараз знаходиться в Національному Музеї комп'ютерів в Блетчлі-Парк.



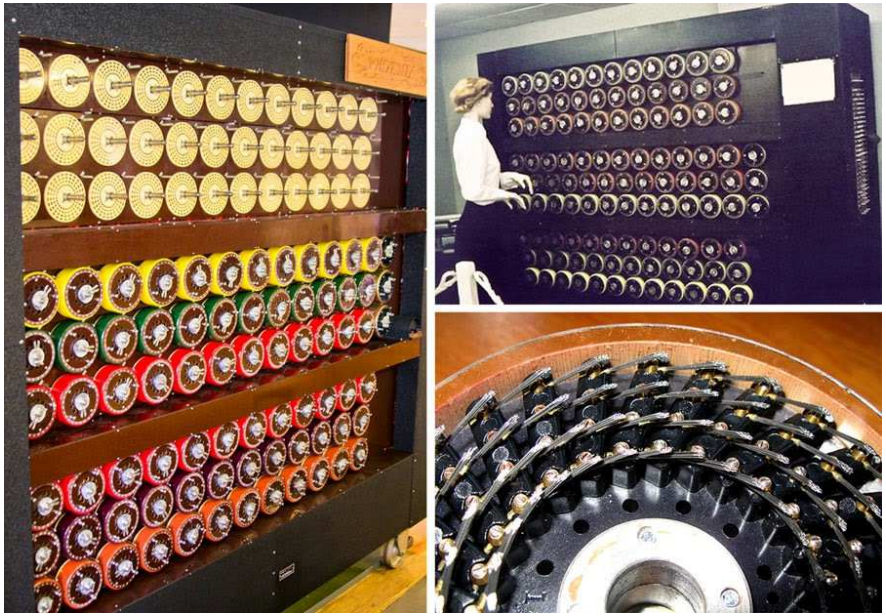


COLOSSUS

Colossus використовував 1500 електронних ламп, будучи на той момент найбільшим комп'ютером у світі, і дозволяв обробляти 5000 знаків за секунду, а, отже, розшифрувати повідомлення за 2-3 години. За сучасними мірками його продуктивність ідентична процесору з частотою 5,8 МГц, такої потужності звичайні комп'ютери досягли тільки через 40 років.

Ця машина виконувала завдання вдвічі швидше, ніж навіть Pentium випуску 1996 р. Програмування правда здійснювалося на примітивному рівні, за допомогою перемикачів і електричних провідників, вони замикали певні контакти на спеціальних панелях. За допомогою Colossus в 1944 році був зламаний шифрувальний код передачі повідомлень вищих чинів нацистської Німеччини. Твердження, що Colossus є одним з перших комп'ютерів, не позбавлене підстав, але і повноцінним комп'ютером цей пристрій все-таки не був, хоча в ньому були електронні схеми, які виконували цифрові функції. Електронної пам'яті він не мав, дані зберігалися на замкнутій перфострічці. Така стрічка рухалася зі швидкістю 80 км/год і дозволяла комп'ютеру зчитувати тільки 5000 символів за секунду.

Bombe – електронно-механічна дешифрувальна машина, створена в роки Другої світової війни за участі британського математика Алана Тьюрінга для розшифровки повідомлень, зашифрованих за допомогою німецької машини Enigma.



Принцип роботи Bombe полягав у переборі можливих варіантів ключа шифру і спроб розшифровки тексту за допомогою відомої структури зашифрованого повідомлення. Важила така конструкція 2,5 тонни, габарити: довжина – 3м, висота – 2,1м, ширина – 0,61м. У Блетчлі-Парк військового часу було встановлено 212 машин типу Bombe, що дозволяло розшифровувати до 3 тис. повідомлень в день. Після війни були знищені всі Bombe. Лише через 60 років ця машина була відновлена і на це пішло 10 років роботи. Для цього протягом 2 років збирали докладні креслення і описи до них. Криптоаналітична машина Bombe – британська відповідь на німецьку Enigma.

Раджу подивитися на цю тему фільм «Гра в імітацію» (доступний онлайн українською мовою: https://kino4ua.net/961-gra-v-mtacyu.html)

Додаток

	абвгґдеєжзиіїйклмнопрстуфхцчшщьюя
а	абвгґдеєжзиіїйклмнопрстуфхцчшщьюя
б	бвгґдеєжзиіїйклмнопрстуфхцчшщьюяа
в	вгґдеєжзиіїйклмнопрстуфхцчшщьюяаб
г	гґдеєжзиіїйклмнопрстуфхцчшщьюяабв
ґ	ґдеєжзиіїйклмнопрстуфхцчшщьюяабвг
д	деєжзиіїйклмнопрстуфхцчшщьюяабвгґ
е	єжзиіїйклмнопрстуфхцчшщьюяабвгґд
є	жзиіїйклмнопрстуфхцчшщьюяабвгґде
ж	зиіїйклмнопрстуфхцчшщьюяабвгґдеє
з	иіїйклмнопрстуфхцчшщьюяабвгґдеєж
и	іїйклмнопрстуфхцчшщьюяабвгґдеєжз
і	їйклмнопрстуфхцчшщьюяабвгґдеєжзи
ї	йклмнопрстуфхцчшщьюяабвгґдеєжзиі
й	клмнопрстуфхцчшщьюяабвгґдеєжзиії
к	лмнопрстуфхцчшщьюяабвгґдеєжзиіїй
л	мнопрстуфхцчшщьюяабвгґдеєжзиіїйк
м	нопрстуфхцчшщьюяабвгґдеєжзиіїйкл
н	опрстуфхцчшщьюяабвгґдеєжзиіїйклм
о	прстуфхцчшщьюяабвгґдеєжзиіїйклмн
п	рстуфхцчшщьюяабвгґдеєжзиіїйклмно
р	стуфхцчшщьюяабвгґдеєжзиіїйклмноп
с	туфхцчшщьюяабвгґдеєжзиіїйклмнопр
т	уфхцчшщьюяабвгґдеєжзиіїйклмнопрс
у	фхцчшщьюяабвгґдеєжзиіїйклмнопрст
ф	хцчшщьюяабвгґдеєжзиіїйклмнопрсту
х	цчшщьюяабвгґдеєжзиіїйклмнопрстуф
ц	чшщьюяабвгґдеєжзиіїйклмнопрстуфх
ч	шщьюяабвгґдеєжзиіїйклмнопрстуфхц
ш	щьюяабвгґдеєжзиіїйклмнопрстуфхцч
щ	ьюяабвгґдеєжзиіїйклмнопрстуфхцчш
ь	юяабвгґдеєжзиіїйклмнопрстуфхцчшщ
ю	яабвгґдеєжзиіїйклмнопрстуфхцчшщь
я	абвгґдеєжзиіїйклмнопрстуфхцчшщью

Таблиця Віженера. Буква $x + y$ знаходиться на перехресті рядка, що відповідає букві x, і стовпчика, що відповідає букві y.