«КРИПТОГРАФІЯ ТА СТЕГАНОГРАФІЯ»

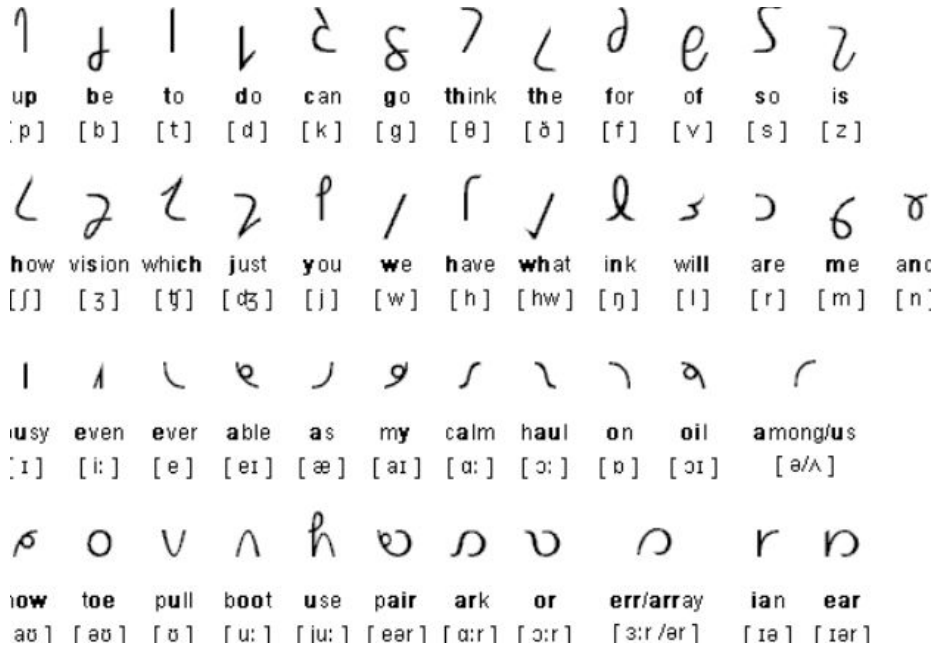
ВСТУП ДО ФАХУ

Лекція 13

Навіщо люди кодують інформацію?

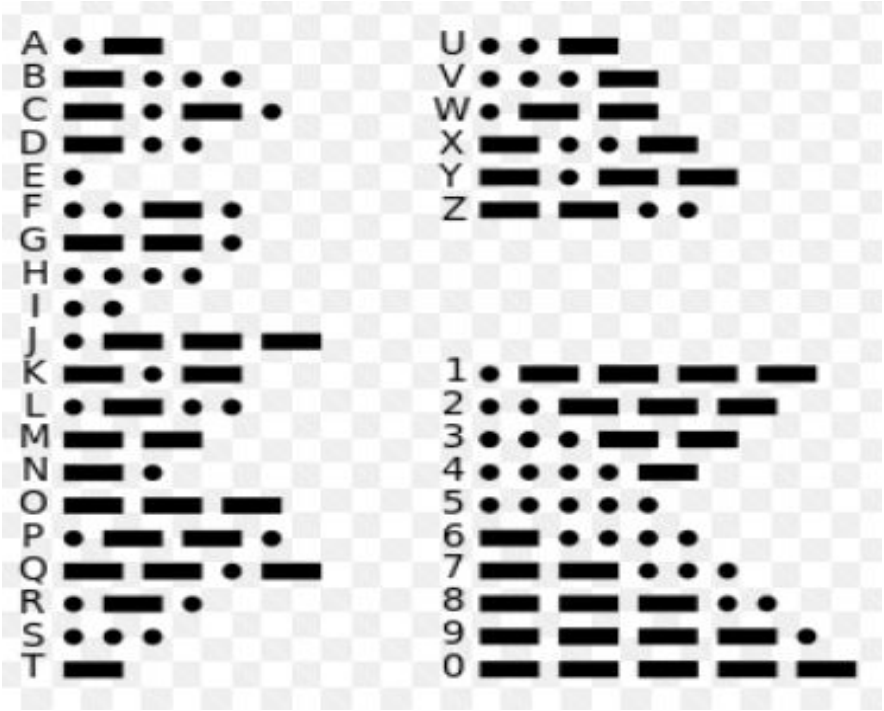
1) Щоб приховати її від інших
(дзеркальна тайнопис Леонардо да Вінчі, військові шифровки),

2) Щоб записати інформацію коротше
(стенографія, абревіатура, дорожні знаки),



ВУЗ	ВВП	МЧС
НЛО	США	ГТО

3) Щоб її було легше обробляти і передавати (азбука Морзе, машинні коди).



Криптографія

(від грец. Κρυπτός - прихований і γράφω - пишу)

- наука про методи забезпечення:

1. конфіденційності (неможливості прочитання інформації стороннім),
2. цілісності даних (Неможливості непомітного зміни інформації),
3. аутентифікації (перевірки справжності авторства або інших властивостей об'єкта) шифру

Термінологія

Криптоаналіз - наука, що вивчає математичні методи порушення конфіденційності та цілісності інформації.

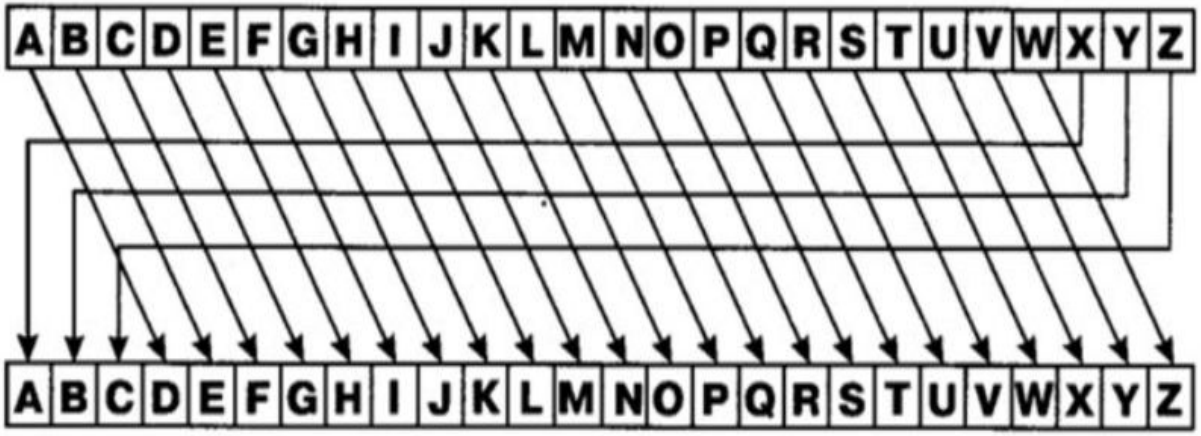
Криптографія і криптоаналіз складають **криптологію**, цілу науку про створення і зломі шифрів (такий розподіл привнесено з заходу).

Криптографічна стійкість-здатність криптографічного алгоритму протистояти криптоанализу.

Криптографічна атака - спроба криптоаналитика викликати відхилення в захищеній системі обміну інформацією. Успішну криптографічний атаку називають **взлом**.

Початок криптографії, в своєму сучасному розумінні цього слова, пов'язане з Юлієм Цезарем.

«Шифр Цезаря» - спосіб, яким Юлій Цезар ховав свої записи від надто цікавих глаз. С висоти досягнення сучасної критики шифр Цезаря представляється примітивним: у ньому кожна буква повідомлення замінюється на наступну за нею за алфавітом, або через три знаки. Однак для того часу, коли вміння читати і писати було рідкісним винятком, його криптостійкості цілком вистачало.



У 15-16 століттях

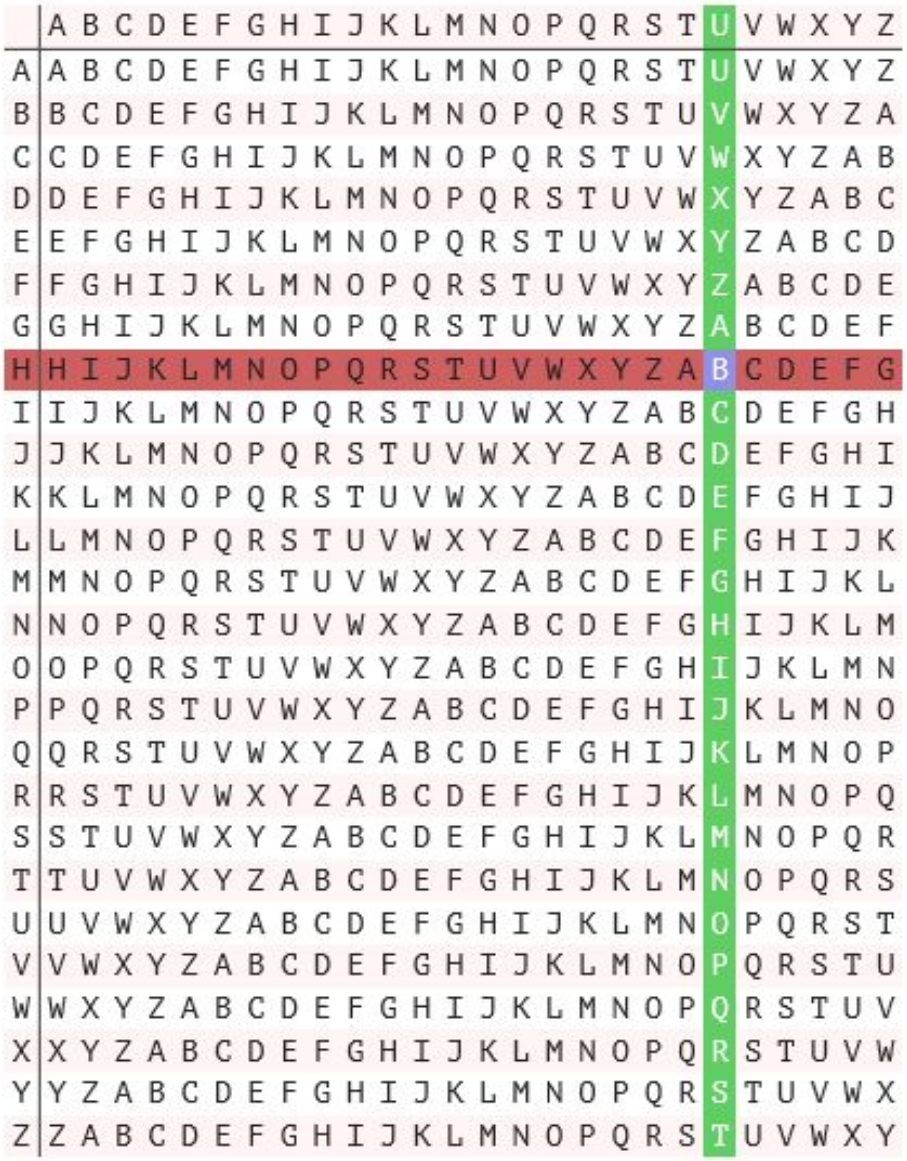
були вперше описані **поліалфавітні шифри** - наступний етап у розвитку криптографії. Ідея полягала в тому, щоб для кожної наступної букви перемикати алфавіт, на який відбувається підстановка, на інший. Найвідомішим виявився **шифр Віженера,** який поєднує кілька шифрів Цезаря з різними значеннями зсуву. Для шифрування потрібна квадратна таблиця алфавітів (tabula recta), ключ (ключове слово) і вихідний текст.

Ключ: HELLO

Текст: USERFRIENDLY

Ключ HELLOHELLOHE
Откр.текст USERFRIENDLY
Шифротекст BWPCTYMPYRSC

↑ Наведите мышку / нажмите пальцем :)



Ключ: HELLO

Текст: USERFRIENDLY

Ключ	HELLOHELLOHE
Откр.текст	USERFRIENDLY
Шифротекст	BWPCTYMPYRSC

↑ Наведите мышку / нажмите пальцем :)

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Ключ: HELLO

Текст: USERFRIENDLY

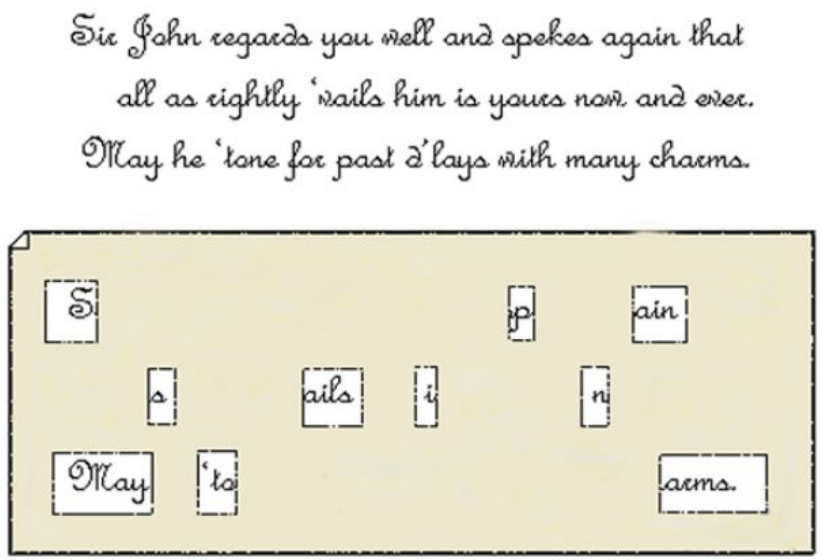
Ключ	HELLOHELLOHE
Откр.текст	USERFRIENDLY
Шифротекст	BWPCTYMPYRSC

↑ Наведите мышку / нажмите пальцем :)

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

1828 Решітка Кардано

Шифратор поміщає решітку на аркуш паперу і пише повідомлення в прямокутних отворах, в яких міститься окремий символ, склад або ціле слово. Оригінал тексту виявляється розділеним на велике число маленьких фрагментів. Потім решітка забирається, і порожні місця на папері заповнюються стороннім текстом так, щоб приховуваний текст став частиною іншого тексту.



1926 рік

- саме в цьому році **Німеччина вперше застосувала в військовій справі шифрувальні машини**. Це стало своєрідним поштовхом для інших країн в розробці і розвитку власних методів шифрування і дешифрування. Першість в теоретичних розробках машин належить полякам і французам, англійці продовжили криптологічний аналіз після окупації Польщі та Франції.

«Енігма»

Історія найвідомішої електричної роторної шифрувальної машини - «Енігма» - починається в 1917 році - з патенту, отриманого голландцем Хьюго Кохом

.

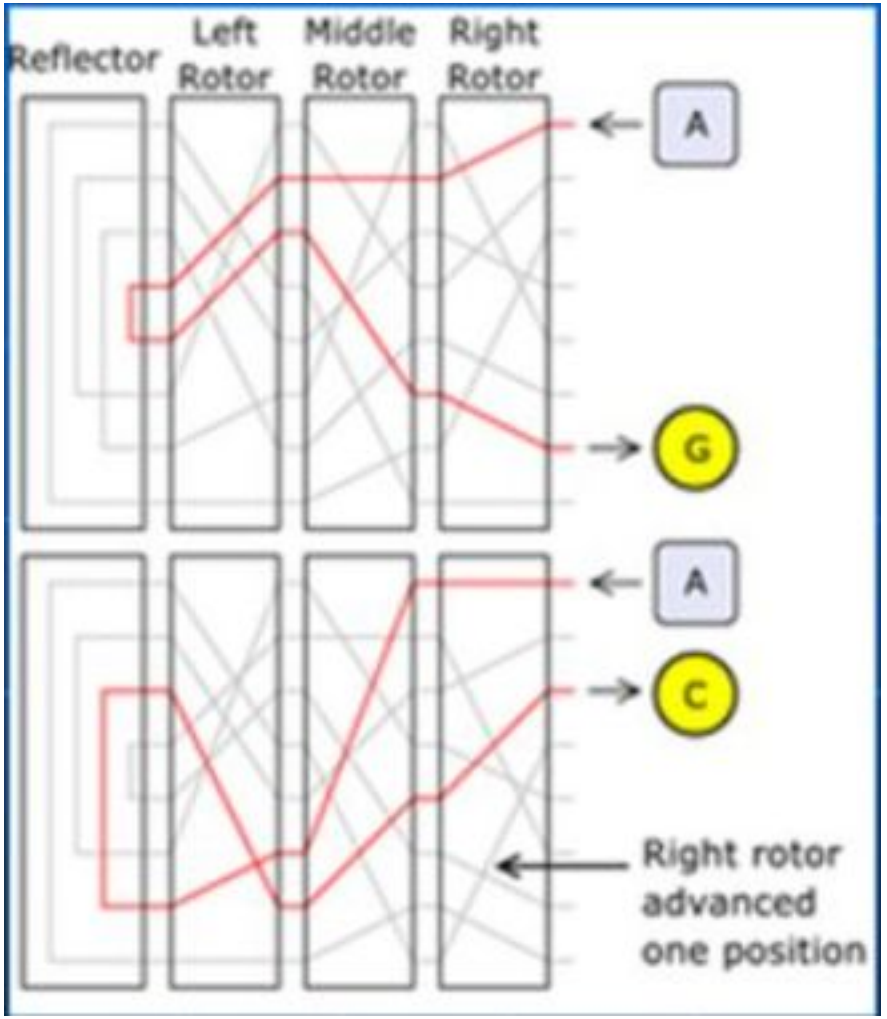
В кінці 1920-х - початку 1930 років, не дивлячись на передані німецьким аристократом Хансом Тіло-Шмідтом дані по машині, що були екземпляри комерційних варіантів, британська і французька розвідка не стали братися за задачу кріптоаналіза. К тому часу вони вже визнали, що шифр є незламним.

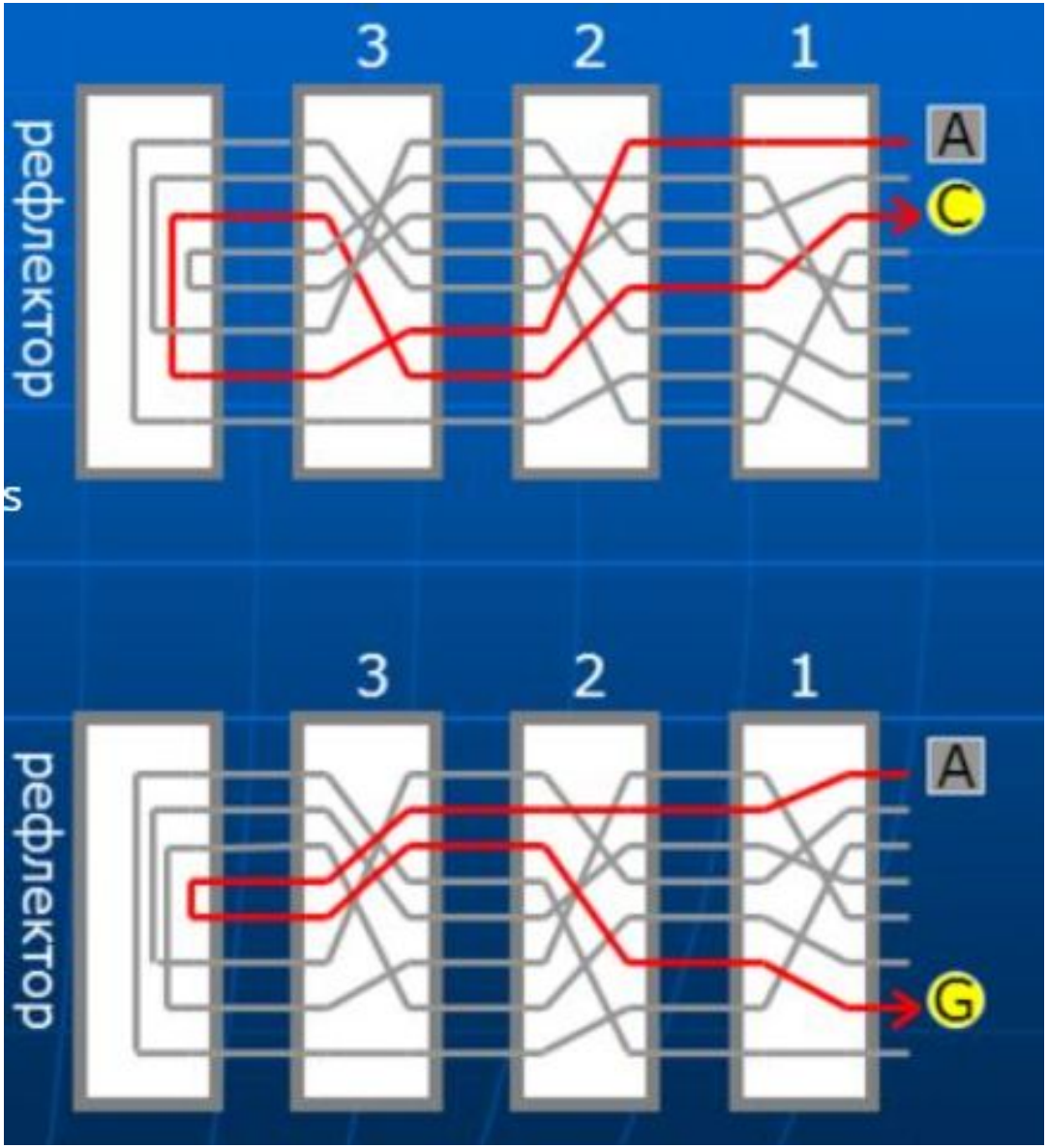
Ротор - диск, який має з кожного боку 26 контактів Всередині ротора контакти попарно з'єднані.

Контакти сусідніх роторів торкаються один одного, створюючи тим самим електричне коло

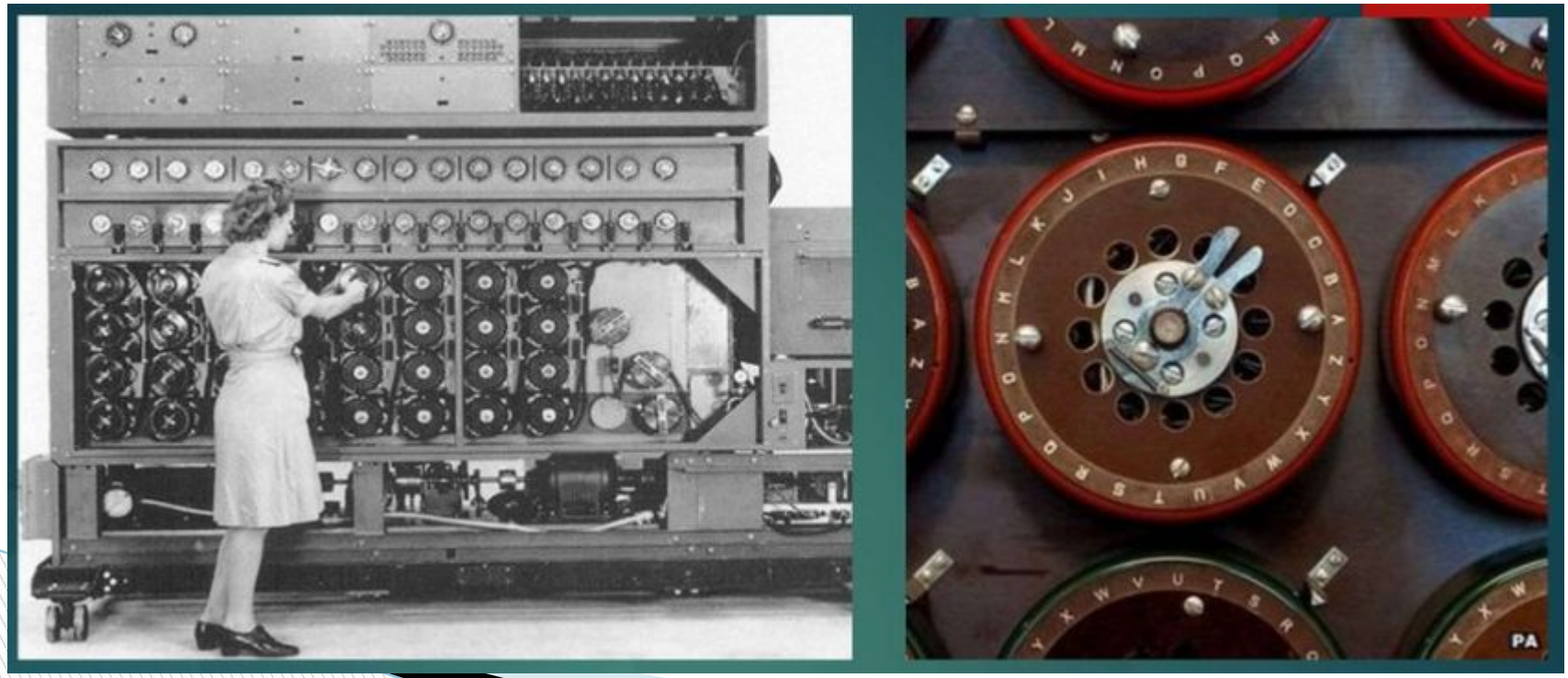
Зашифрована 1-м ротором буква шифрується 2-м ротором, далі - 3-м, потім проходить через рефлектор, шифрується знову 3-м, потім 2-м і 1-м.

Коли буква зашифрована, ротори повертаються за певним алгоритмом. В результаті, одна і та ж буква шифрується різними символами.



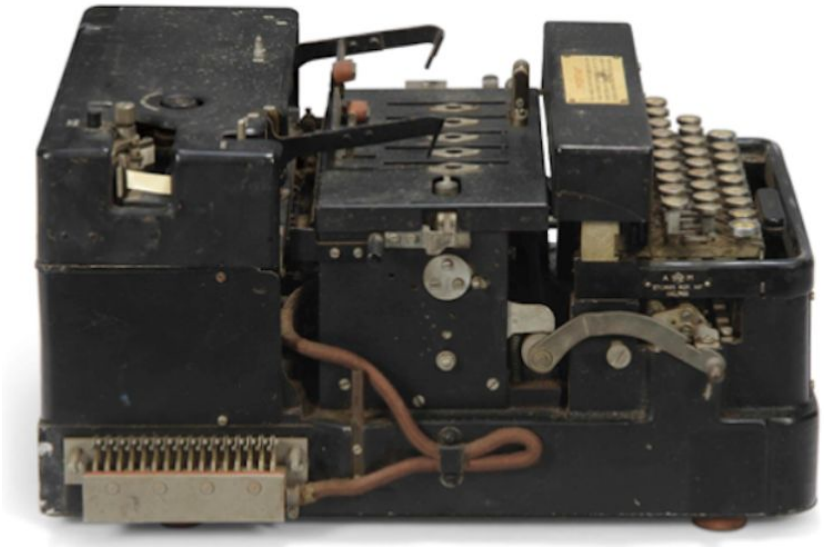

3
2
1
A
C
рефлектор
s
3
2
1
A
G
рефлектор

Розроблений під керівництвом Алана Тьюринга і Джоан Кларк дешифратор. Його використання дозволило союзникам розколоти здававшийся монолітним код «Енігми».



Турех —

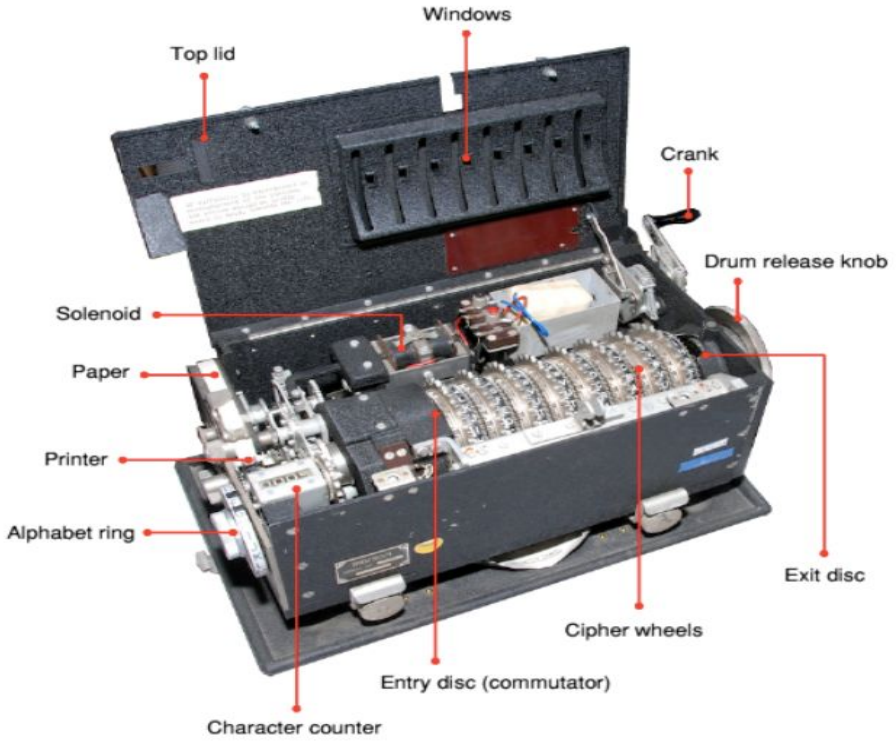
електромеханічна роторна шифрувальна машина, розроблена в Великобританії в 1934 році.



Відразу за клавіатурою знаходився роторний барабан (кошик), в якому розміщувалися п'ять роторних коліс. Клавіатура і роторна кошик - два елементи машини, що є копією німецької **Енігми**.

Portex BID / 50/1

Portex представляла собою британську електромеханічну кріпто-машіну, яка використовувалася секретними службами Великобританії в 1940 і 1950 роках. Машина схожа на німецьку Енігму, правда в її розпорядженні було 8 роторів з 26 контактами кожен.



Сучасні методи використання криптографії

Поява доступного інтернету перевело криптографію на новий рівень. Криптографічні методи стали широко використовуватися приватними особами в електронних комерційних операціях, телекомунікації та багатьох інших середовищах. Перша отримала особливу популярність і привела до появи нової, не контролюється державою валюти - **біткойнов.**

Багато ентузіасти швидко зметикували, що банківський переказ - штука, звичайно, зручна, однак, для покупки таких приємних в побуті речей, як зброю, він не підходить. Не підходить він і при запущених випадках параної, бо вимагає від одержувача і відправника обов'язкової аутентифікації.

Уже в 2009 році Сатоши Накамото (якого багато хто свято вважають цілої хакерської угрупованням) розробив платіжну систему нового типу - BitCoin. Так народилася **криптовалюта**.

Її транзакції не вимагають посередника у вигляді банку чи іншої фінансової установи, відстежити їх неможливо. Мережа повністю децентралізована, біткойни не можуть бути заморожені або вилучені, вони повністю захищені від державного контролю.

У той же час біткойн може використовуватися для оплати будь-яких товарів - за умови згоди продавця.

Квантові комунікації (чи квантова криптографія)

-технологія кодування і передачі даних в квантових станах фотонів.

Закони фізики не дозволяють виміряти квантовий стан так, щоб воно не змінилося, тому квантовий канал зв'язку неможливо прослухати непомітно для адресатів.

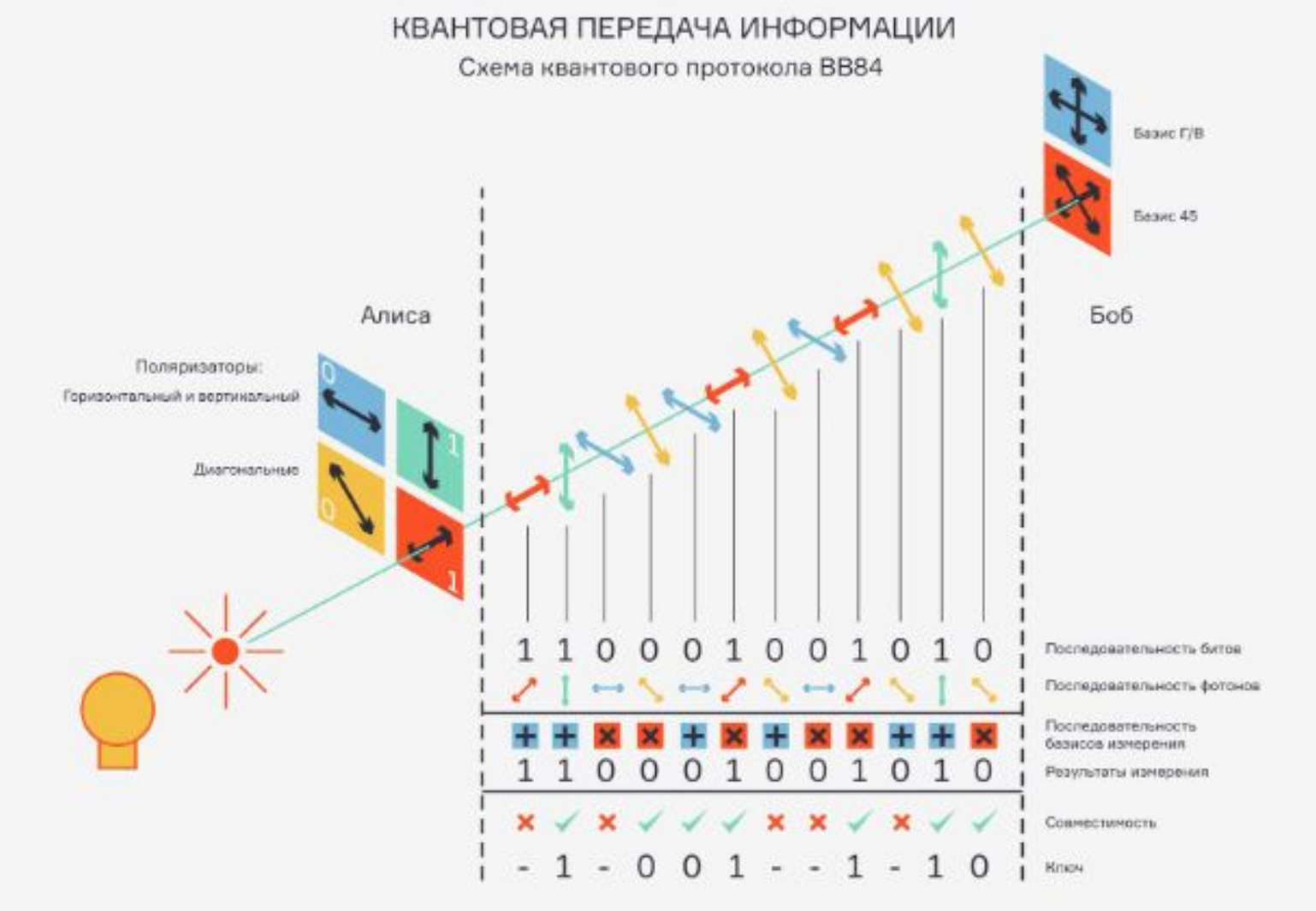
Квантові комунікації і квантові мережі сьогодні активно розвиваються у всьому світі, вони затребувані банками, державними організаціями і військовими.

Квантові комунікації (чи квантова криптографія)

дані кодуються в станах фотона, які відповідно до законів квантової механіки безповоротно міняються при спробі виміру.

У теорії для квантового зв'язку можна використати будь-які об'єкти, здатні знаходитися в двох різних квантових станах, інакше кажучи, будь-які **кубіти** - електрони, іони і так далі. Проте через широке розповсюдження волоконно-оптичних мереж **фотони** залишаються практично безальтернативним варіантом для квантової криптографії.

У звичайних волоконних лініях інформація кодується в імпульсах випромінювання лазера, наприклад в дворівневій формі (є сигнал - 1, немає сигналу - 0). Для квантового зв'язку дані кодуються в станах поодиноких фотонів - наприклад, в поляризації або фазі. Так, одному варіанту поляризації приписується значення 1, протилежному - 0.


КВАНТОВАЯ ПЕРЕДАЧА ИНФОРМАЦИИ
Схема квантового протокола BB84
Базис Г/В
Базис 45
Алиса
Боб
Поляризаторы:
Горизонтальный и вертикальный
Диагональные
1 1 0 0 0 1 0 0 1 0 1 0
Последовательность битов
Последовательность фотонов
Последовательность базисов измерения
1 1 0 0 0 1 0 0 1 0 1 0
Результаты измерения
Совместимость
- 1 - 0 0 1 - - 1 - 1 0
Ключ

Квантові комунікації (чи квантова криптографія)

Два головні учасники квантової бесіди традиційно позначаються як **Аліса** (посилач повідомлення) і **Боб** (одержувач), іноді до цих героїв приєднується третій - **Єва**, яка намагається підслуховувати розмову. Коли Єва вимірює фотони, їх стани міняються, і Боб розуміє, що лінія зв'язку скомпрометована.

Квантові комунікації (чи квантова криптографія)

Головні недоліки квантової криптографії

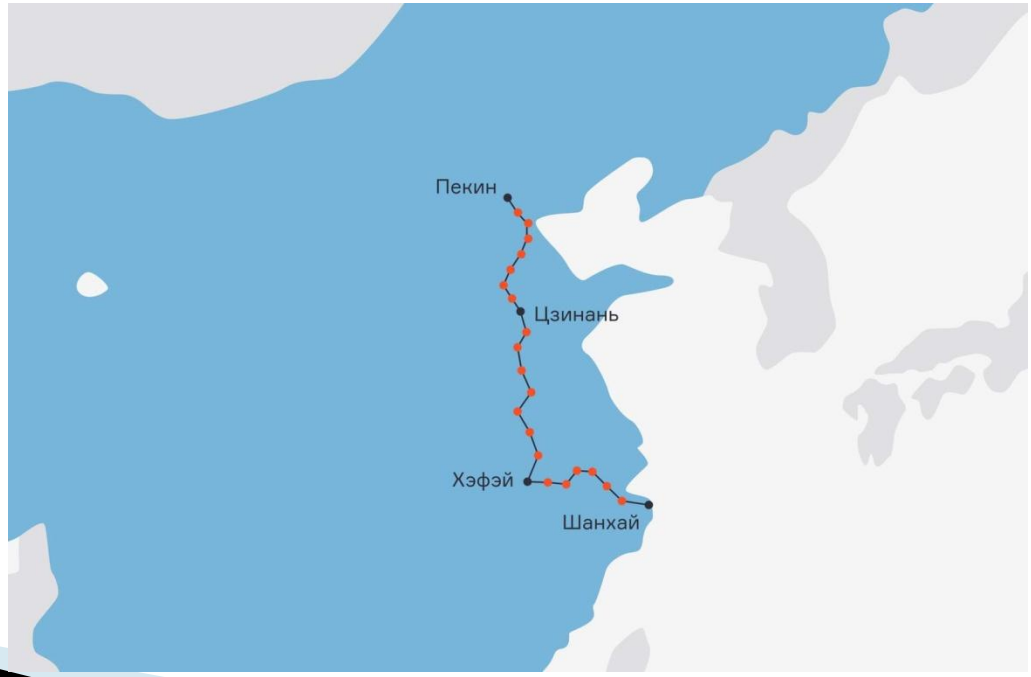
Кодувати дані в квантових станах досить складно, оскільки для цього необхідно уміти генерувати і детектувати поодинокі фотони, що саме по собі непросте технологічне завдання.

Квантові стани уразливі і можуть руйнуватися під дією теплових шумів і інших перешкод.

Квантовий зв'язок сьогодні можливий тільки на обмежених відстанях. Кращі лабораторні зразки квантових систем ледве здолали поріг дальності 400 кілометрів, при цьому вони забезпечують украй низьку за сучасними стандартами швидкість - близько 1 біта в секунду. Тому існуючі квантові мережі в основному забезпечують захищений зв'язок на відстанях в десятки кілометрів.

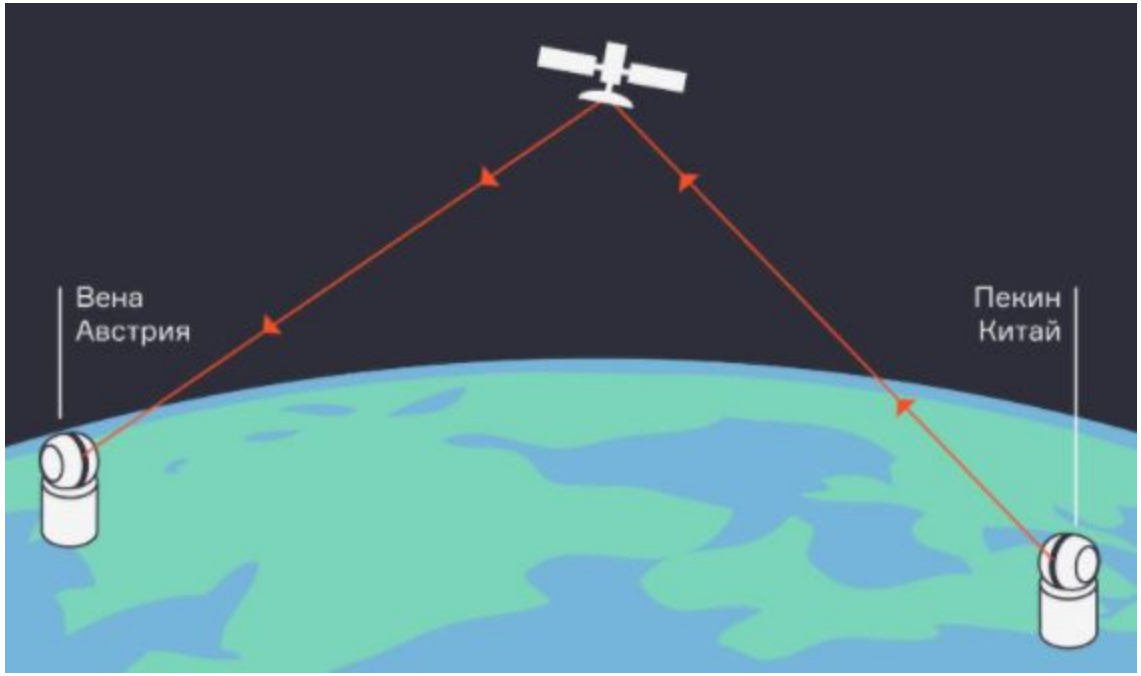
Квантові комунікації (чи квантова криптографія)

Другий варіант - використання космічних технологій : втрати фотонів в атмосфері і космосі відносно невеликі в порівнянні з поглинанням в оптоволокні, тому супутник-ретранслятор може забезпечити квантовий зв'язок на дистанції в тисячі кілометрів.

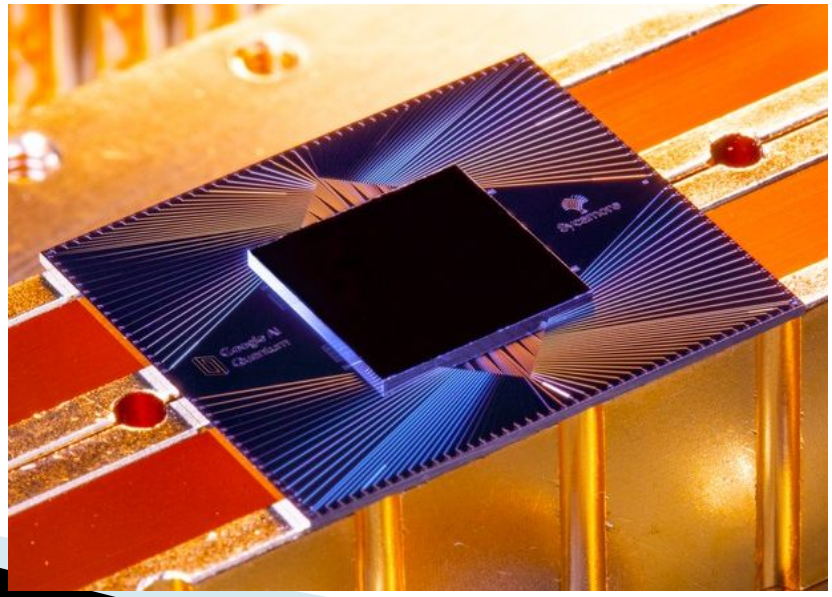


Квантові комунікації (чи квантова криптографія)

У 2017 році китайський супутник "Мо-Цзи" забезпечив розподіл фотонів на рекордну відстань - понад 1200 кілометрів, а пізніше з його допомогою була організована квантова лінія між Віднем і Пекіном.



Позаминулого року компанія Google уперше вирішила завдання, недоступне класичному суперкомп'ютеру, але це завдання дуже далеке від злому криптографічних систем. Більше того, квантовим комп'ютерам буде потрібно не один рік, щоб дійти до рівня, коли можна буде зламати хоч би старі системи, де використовується слабка криптографія. Проте важливо розуміти, що як тільки з'явиться квантовий комп'ютер, вже пізно міняти криптографію, тому стандартизація нових протоколів відбувається зараз..



Стеганографія

(від грец. Στεγανοσ - прихований і грец. Γραφω - пишу, буквально «тайнопис») - наука про захист інформації шляхом приховування факту передачі повідомлення.

Уже в стародавньому світі виділилося два основних напрямки вирішення цього завдання, існуючі і по сьогоднішній день: **криптографія і стеганографія**. Метою криптографії є приховування вмісту повідомлень за рахунок їх шифрування.

На відміну від цього, при стеганографії **ховається сам факт існування таємного повідомлення.** Історично цей напрям з'явилося першим, але потім багато в чому було витіснено криптографією. Тайнопис здійснюється самими різними способами. Спільною рисою цих способів є те, що приховуване повідомлення вбудовується в деякий нешкідливий, не привертаючий увагу об'єкт.

Існують два основних напрямки в комп'ютерної стеганографії: **пов'язана з цифровою обробкою сигналів і не пов'язане.**

В останньому випадку повідомлення можуть бути вбудовані в заголовки файлів, заголовки пакетів даних. Цей напрямок має обмежене застосування в зв'язку з відносною легкістю розтину і / або знищення прихованої інформації. Більшість поточних досліджень в області стеганографії, так чи інакше, пов'язані з цифровою обробкою сигналів. Це дозволяє говорити про цифрову стеганографію.


КЛАСИЧНА СТЕГАНОГРАФІЯ
Хімічні методи
Фізичні методи
Симпатичні хімікалії
Органічні рідини
Схованки
Камуфляж
Мікрокрапки
Голограми

Цифрова стеганографія

це галузь знань та технічна наука, яка розглядає методи:

– організації прихованих каналів передачі і зберігання інформації з використанням різних цифрових об’єктів (засобів і систем зберігання і передачі електронної інформації);

– вбудовування спеціальних міток в електронну інформацію з метою захисту від підробки та несанкціонованого тиражування (цифрових водяних знаків – електронних голографічних елементів).

Цифрова стеганографія

сучасна прикладна стеганографія узагальнює такі поняття, як:

- сховище (тайник) та **контейнер** (засіб зберігання чи передачі прихованої інформації);

– **тайникова операція** (порядок обміну повідомленнями через сховище);

– **сигнальна інформація** (порядок обміну повідомленнями про небезпеку чи безпеку особистого контакту; знак підтвердження або спростування факту відсилання чи отримання кореспонденції, матеріальних і технічних засобів тощо);

– **канал передачі/витоку/несанкціонованого доступу** (стеганографічний канал передачі/зберігання інформації шляхом використання стеганограм, тобто заповнених контейнерів, що містять приховану інформацію).

Цифрова стеганографія

У загальному випадку всі методи стеганографії використовують деякий **надлишок** в обраній для зміни інформації, за рахунок якого приховується необхідна інформація, і це не призводить до суттєвої зміни властивостей контейнера (дискретного об’єкта) та порушення його функціональності (цільового призначення).

У свою чергу, методи стеганографічного аналізу використовують імовірнісно-статистичні відхилення властивостей стеганограми від контейнера (дискретного об’єкта з прихованою інформацією від його природного стану), що йому відповідає або може відповідати із деякою ймовірністю.


Секретне повідомлення
Блок шифрування
Зображення контейнер
Алгоритм вбудовування
Заповнений контейнер

Цифрова стеганографія

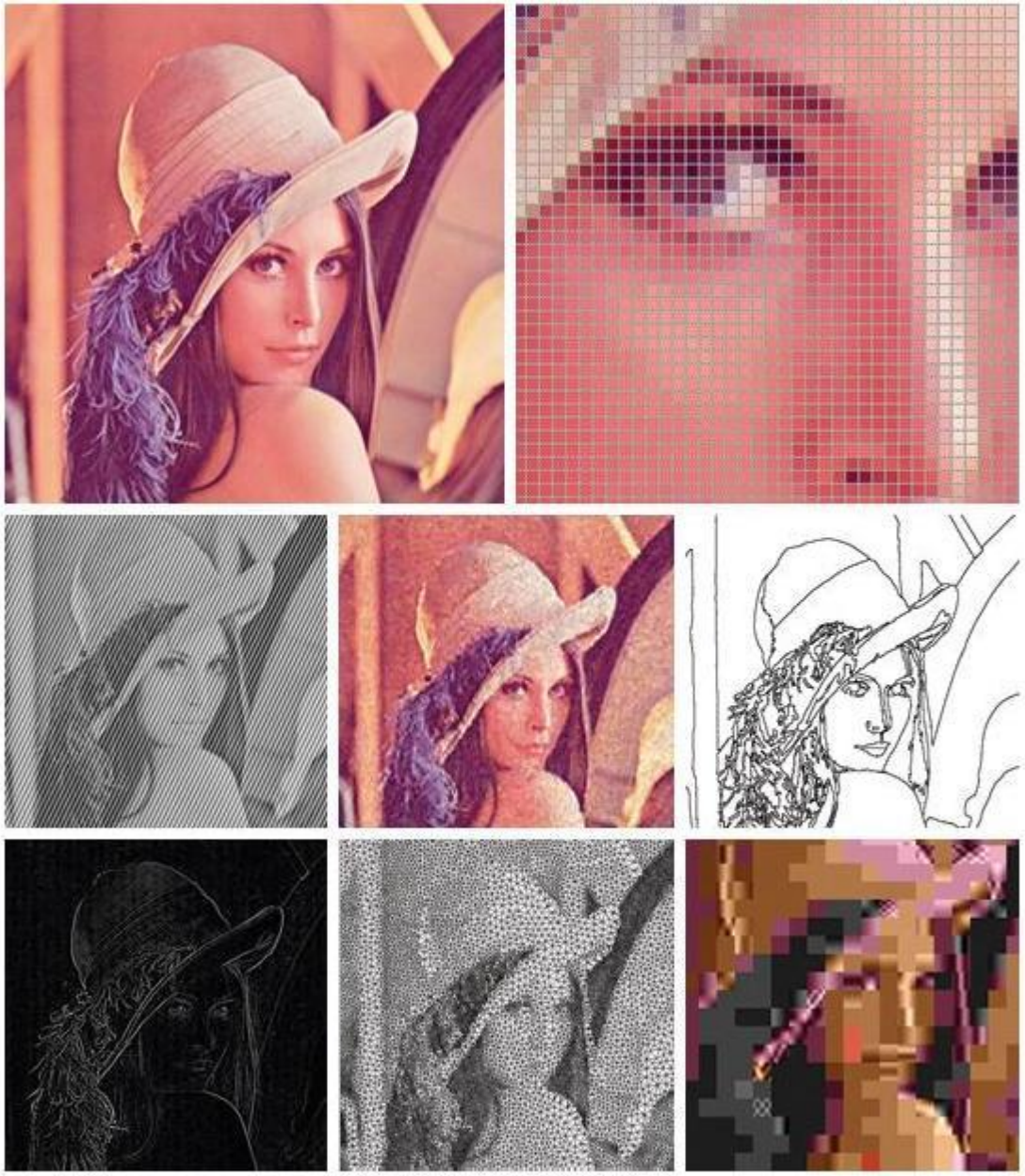
У якості контейнера (повідомлення) може використовуватися будь-яка інформація призначена для приховування таємних повідомлень.

Повідомленням може бути як текст або зображення, так і, наприклад, аудіодані (файли мультимедіа) тощо. Порожній контейнер – контейнер без вбудованого повідомлення; заповнений контейнер (стег) – контейнер, що містить вбудовану інформацію. Вбудоване (приховане) повідомлення – повідомлення, вбудовується в контейнер. Стеганографічний канал або просто стегоканал – канал передачі стег. Стегоключ або просто ключ – секретний ключ, необхідний для приховування інформації. В залежності від кількості рівнів захисту (наприклад, вбудовування попередньо зашифрованого повідомлення) в стегосистеми може бути один або декілька стегоключів.

Приховування впроваджуваних даних, які в більшості випадків мають великий обсяг, пред'являє серйозні вимоги до контейнера: розмір контейнера в кілька разів повинен перевищувати розмір вбудовуваних даних.

Цифрові водяні знаки використовуються для захисту авторських або майнових прав на цифрові зображення, фотографії чи інші оцифровані твори мистецтва. Основними вимогами, які пред'являються до таких вбудованим даними, є надійність і стійкість до спотворень.

Заголовки використовується в основному для маркування зображень у великих електронних сховищах (бібліотеках) цифрових зображень, аудіо-і відеофайлів.



Отже, стегосистема має відповідати таким вимогам:

1) властивості контейнера повинні бути модифіковані таким чином, щоб зміни неможливо було виявити при візуальному контролі, що визначає якість приховування повідомлення (для безперешкодного проходження стегоповідомлення каналами зв'язку воно не повинно привернути увагу);

2) стегоповідомлення повинно бути стійким до спотворень, в тому числі і до зловмисних (у процесі передачі зображення, звука або використання інших контейнерів можуть відбуватися різні трансформації зі зменшення або збільшення, перетворення в інший формат, ущільнення, в тому числі і з використанням алгоритмів з втратою даних тощо);

3) для збереження цілісності вбудованого повідомлення необхідно використовувати коди з виправленням помилок;

4) для підвищення надійності вбудоване повідомлення має бути продубльоване.