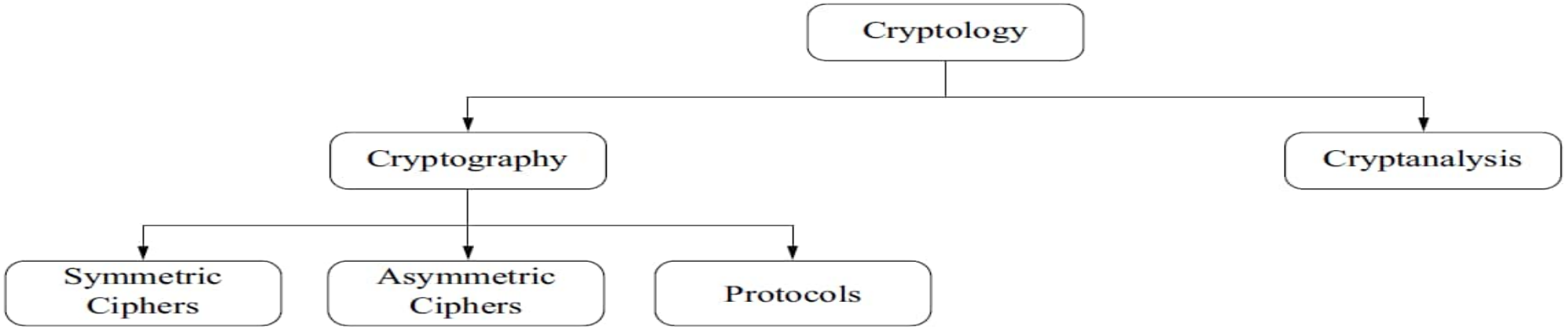
Математична криптологія

Основні поняття та приклади

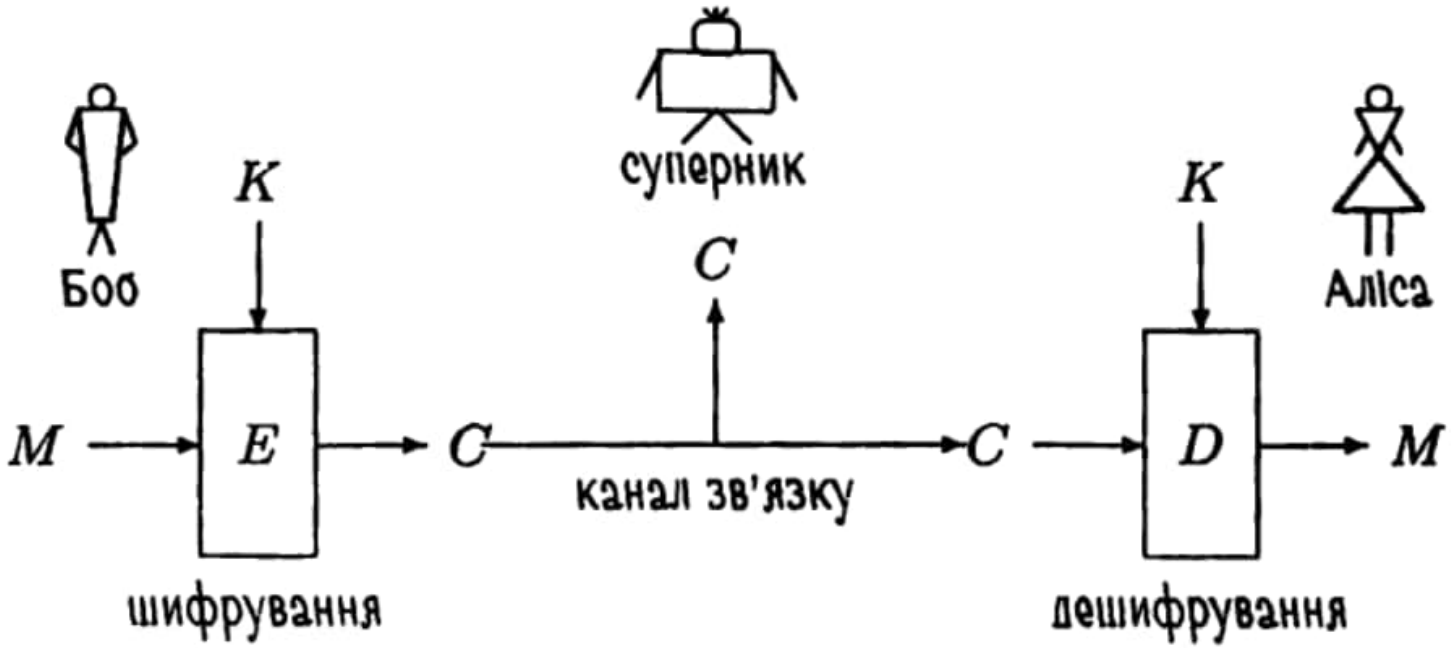
Основні поняття

- **Криптологія (Cryptology) —** це галузь знань, що вивчає тайнопис (криптографію), і методи її розкриття (криптографічний аналіз). Назва криптології пішла від грецької мови (криптос — таємний, логос — наука або слово).
- **Криптографія (Cryptography) —** наука про збереження таємниці тексту.
- **Криптографічний аналіз (Cryptoanalysis) -** наука про проникнення у таємницю захищеного тексту.
- **Тайнопис** також є ширшим поняттям.
- Вживання **код** та **кодування** як синонімів до **шифру** та **шифрування** є помилковим.



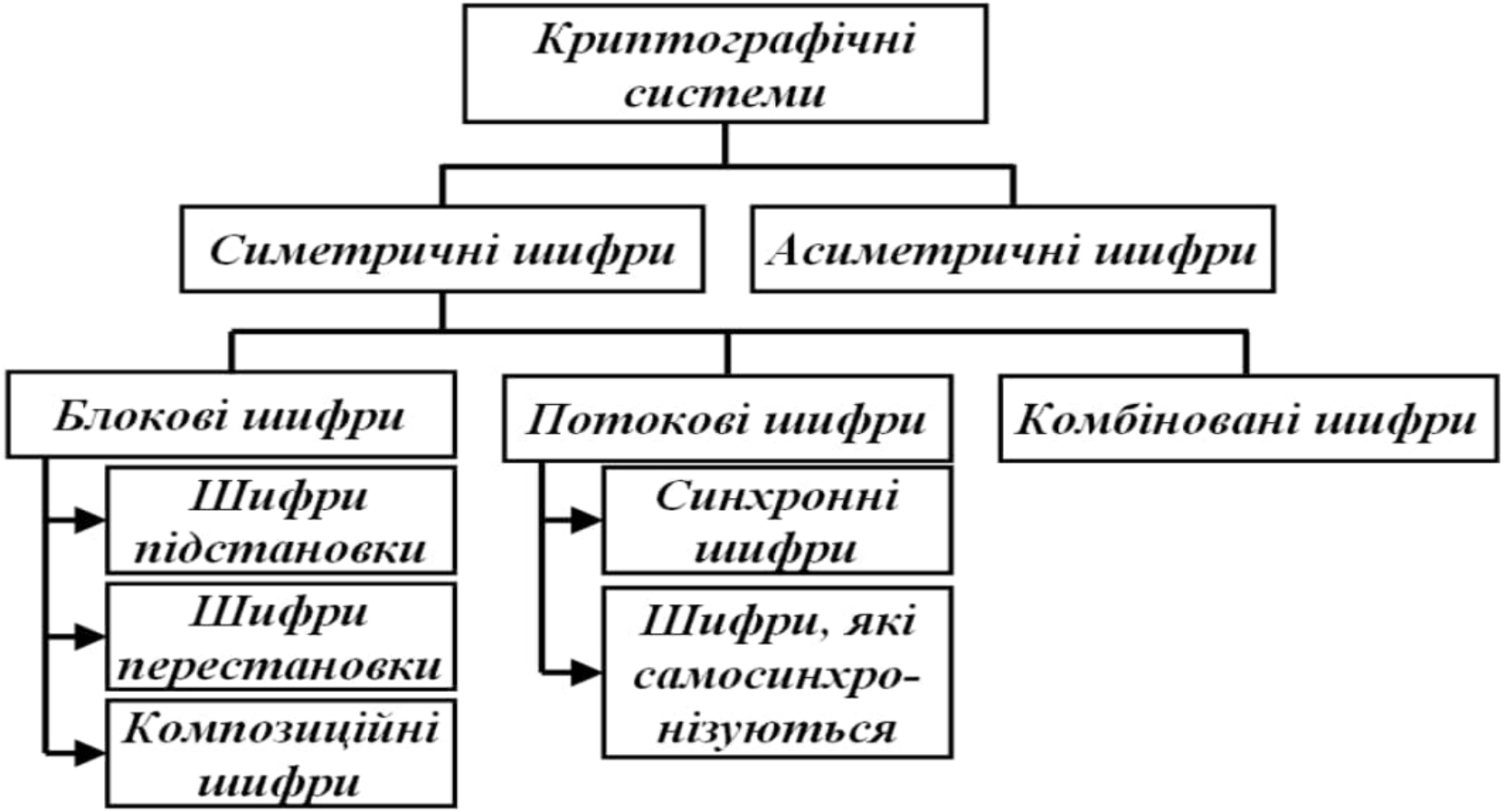
Класична криптографічна схема

- **K (key) –** секретний ключ;
- **E (encryption) –** функція шифрування $C = E_K(M)$;
- **D (decryption) –** функція дешифрування: $M = D_K(C)$;



Симетрична криптосистема

Класифікація методів шифрування

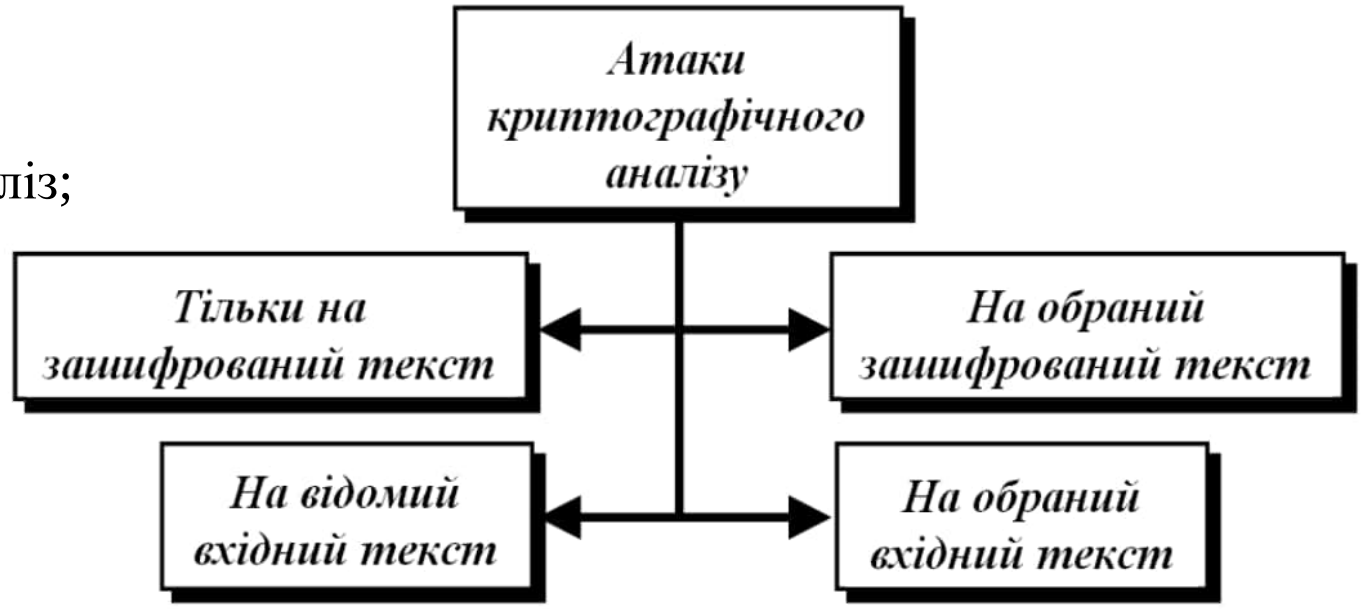


Криптографічна стійкість

- Абсолютно надійний шифр не піддається криптоаналізу;
- Шифр вважається надійним в обчислювальному сенсі, якщо його розкриття хоча в принципі можливе, але навіть на найшвидшемо комп’ютері вимагатиме нереального часу (роки, століття, …), після завершення якого будь-яка таємниця стане неактуальною;
- Принцип Керкгоффза (англ. Kerckhoffs's principle) - стійкість криптографічного алгоритму не має залежати від архітектури алгоритму, а має залежати тільки від ключів.

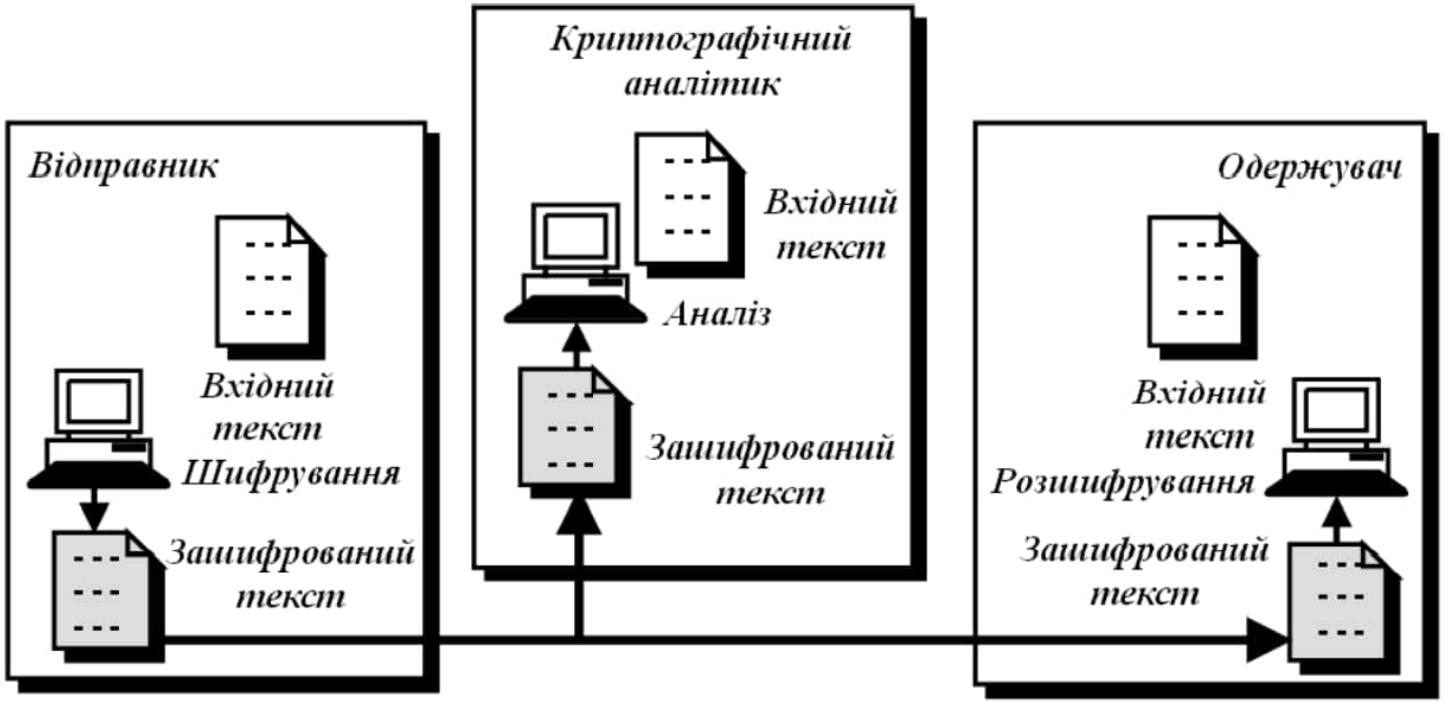
Криптографічний аналіз

- Атака грубої сили (brute force);
- Статистична атака – частотний криптоаналіз;
- Лінійний криптоаналіз;
- Диференціальний криптоаналіз;
- Атака за зразком.



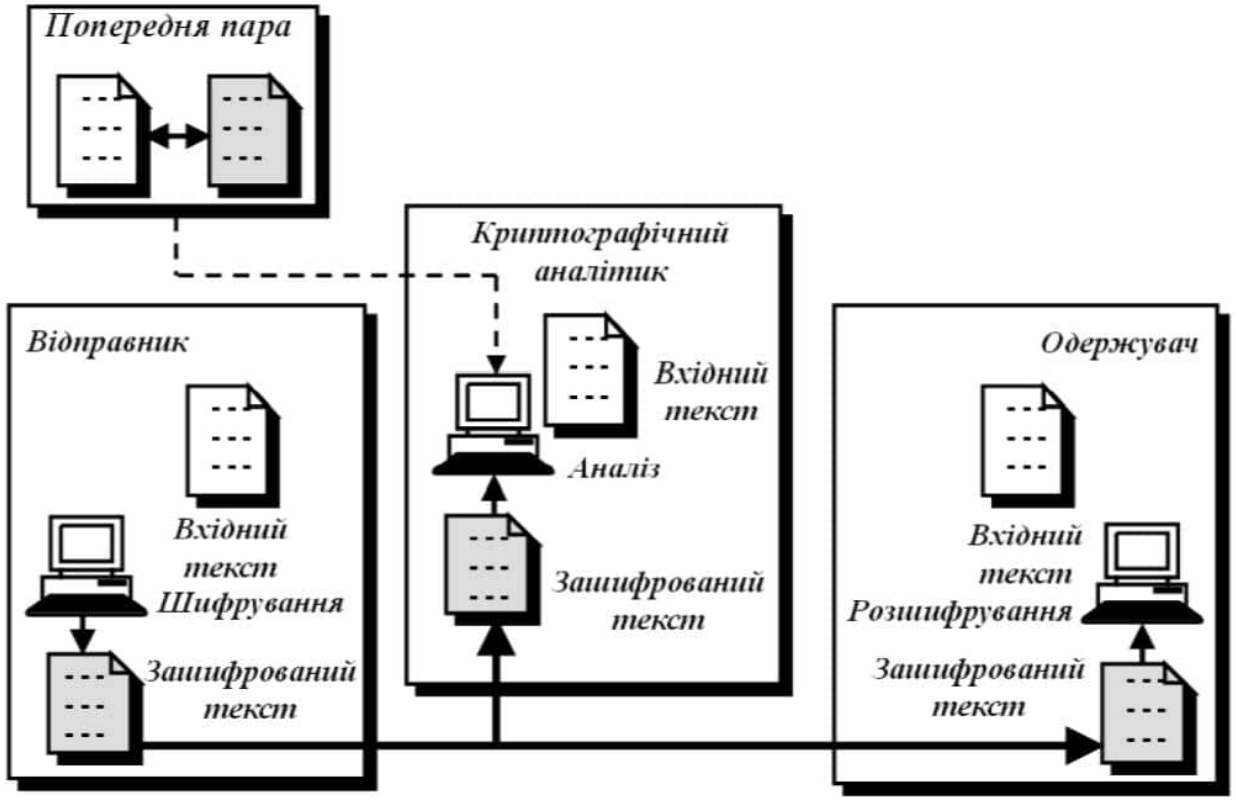
Атака лише із криптотекстом

Суперник знає лише криптотекст $E_K(M)$**,** також відома ще певна кількість криптотекстів $E_K\ (M_1), \ldots, E_K\ (M_l)$, зашифрованих з використанням одного й того ж ключа.



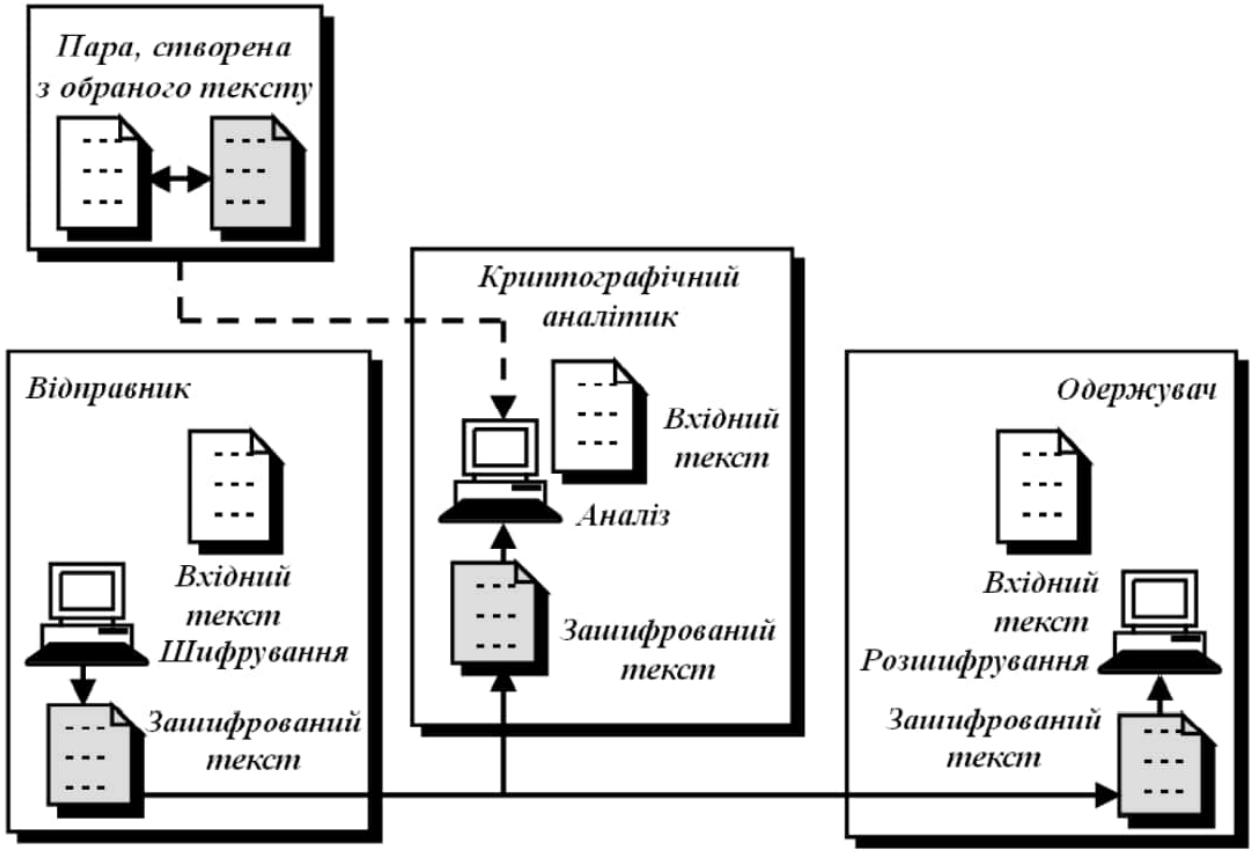
Атака з відомим відкритим текстом

Крім $E_K(M)$ суперник знає як додаткові криптотексти $E_K\ (M_1), \ldots, E_K\ (M_l)$, так і віповідні їм відкриті тексти $M_1, \ldots, M_l$ (які пересилалися раніше і вже не є таємними).



Атака з вибраним відкритим текстом

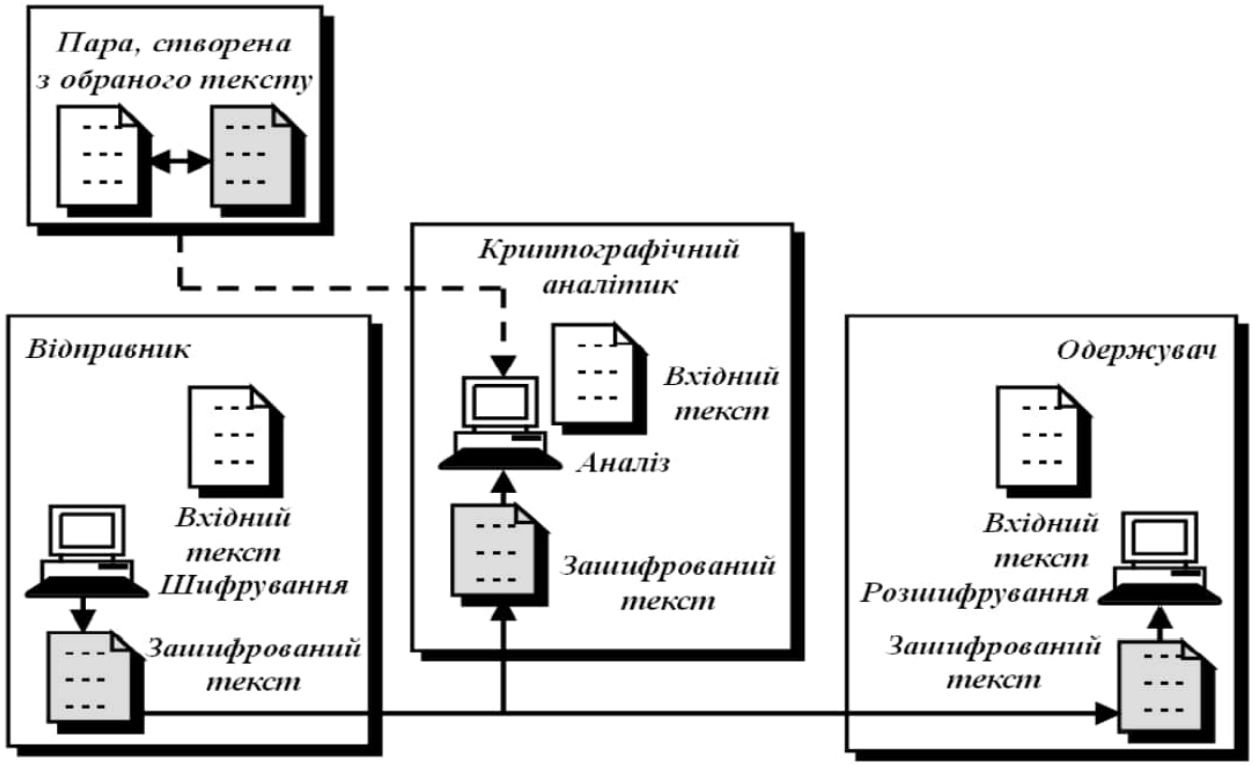
Атака з вибраним відкритим текстом. Суперник має доступ до "шифруючого устаткування" і спроможний отримати криптотексти $E_K(M_1), \ldots, E_K(M_l)$ для вибраних на власний розсуд відкритих текстів $M_1, \ldots, M_l$.



Атака з вибраним криптотекстом

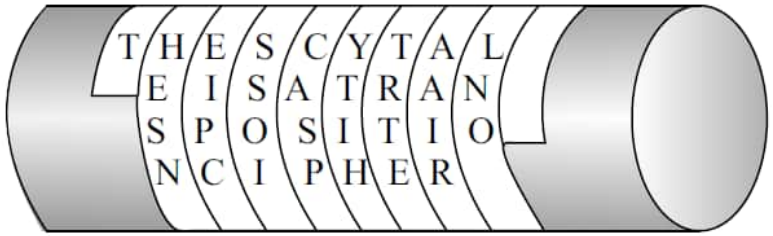
Атака з вибраним криптотекстом. Суперник має доступ до "дешифруючого устаткування" і спроможний отримати відкриті тексти $D_K\ (C_1), \ldots, D_K\ (C_l)$ для вибраних на власний розсуд криптотекстів $C_1, \ldots, C_l$.

Якщо атака певного виду призводить до розкриття шифру, то шифр є вразливим до неї, якщо ж ні, то шифр є стійким до такого виду атаки.

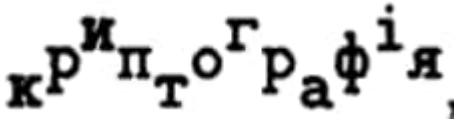


Шифри перестановки

- **Шифр Скитала -** використовувався спартанцями для військових донесень у V ст. до н.е.



- **Шифр частоколу:** криптографія → игірпорфякта



Шифри простої заміни

- **Шифр Ю. Цезаря -** (100 – 44 р. до н.е). Кожна буква алфавіту заміщується циклічним зсувом на 3 позиції вправо: а → г, б → ґ, в → д і т.д.

імперія → лптзулв

- **Частотний криптоаналіз -** У досить довгих текстах кожна буква зустрічається із приблизно однаковою частотою.

пцпспофнпмплпибгпефрптмбвмєоп **охоронумолокозаводупослаблено**

п	0.134	е	0.043	л	0.028	ч	0.011	ї	0.006
о	0.082	р	0.038	у	0.027	б	0.010	є	0.006
н	0.070	і	0.037	п	0.025	х	0.010	ф	0.005
а	0.070	с	0.036	я	0.021	ц	0.009	ш	0.005
и	0.056	к	0.036	э	0.019	ю	0.009	щ	0.003
т	0.051	м	0.033	ь	0.015	ж	0.008	ґ	0.000
в	0.046	д	0.028	г	0.013	й	0.007		

Варто запам’ятати

- **Криптографія це:**

- потужний інструмент для захисту інформації;

- основа для багатьох сек’юрних алгоритмів.

- **Криптографія не вирішує** всіх проблем захисту інформації (fishing).
- **Криптографічні методи надійні**, якщо вони реалізовані та використовуються коректно.
- **Ніколи не намагайтесь винайти власну криптосистему**, оскільки є велика імовірність що не будуть враховані всі фактори криптографічної стійкості та як результат шифр виявиться вразливим.