ЛЕКЦІЯ 1

ЖИТОМИРСЬКА ПОЛІТЕХНІКА
ДЕРЖАВНИЙ УНІВЕРСИТЕТ

Основні поняття та задачі криптології

План

1. Загальні відомості про інформаційну безпеку
2. Основні поняття криптології
3. Класифікація шифрів
4. Застосування криптографії у сучасному світі

1. Загальні відомості про інформаційну безпеку

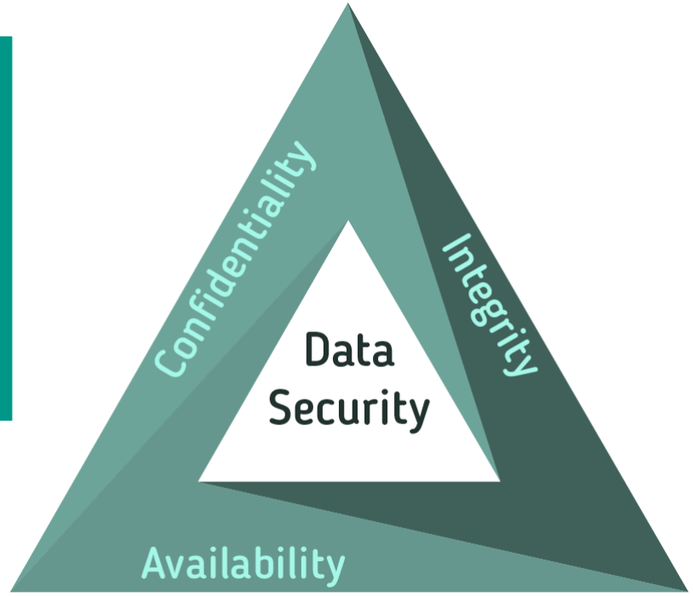
Інформаційна безпека – це стан захищеності систем обробки і зберігання даних, при якому забезпечено конфіденційність, доступність і цілісність інформації

1. Загальні відомості про інформаційну безпеку

Тріада КЦД

Конфіденційність

захист від несанкціонованого ознайомлення зі змістом



Цілісність

неможливість модифікації неавторизованим користувачем

Доступність

отримання даних за вимогою користувача, який має відповідні повноваження

1. Загальні відомості про інформаційну безпеку

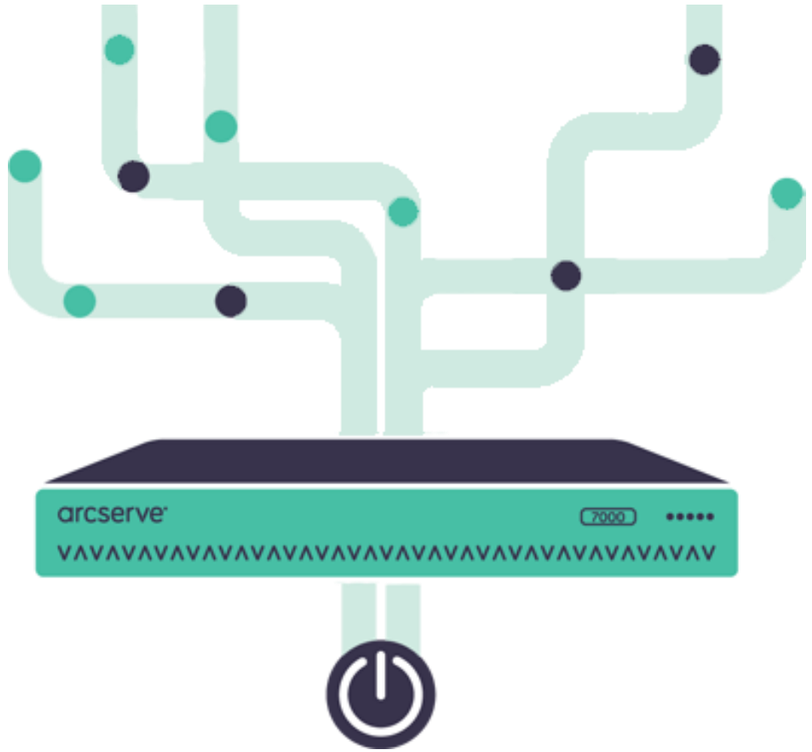
Способи захисту інформації

Фізичні – це засоби, необхідні для зовнішнього захисту обчислювальної техніки, території та об’єктів (охорона, сигналізація, відеоспостереження тощо)

1. Загальні відомості про інформаційну безпеку

Способи захисту інформації

Апаратні – різні за типом пристрої (механічні, електромеханічні, електронні та ін.), які на рівні обладнання вирішують завдання захисту даних (модулі шифрування, апаратне шифрування трафіку, токени безпеки)



1. Загальні відомості про інформаційну безпеку

Способи захисту інформації

Програмні – системні та прикладні програми, призначені для ідентифікації користувачів, розмежування доступу, тестового контролю системи захисту тощо (менеджери паролів, антивірусні програми, файєрволи тощо)

1. Загальні відомості про інформаційну безпеку

Способи захисту інформації

Законодавчі – діючі в країні закони, укази, положення, інструкції та інші нормативні акти, які регламентують правила поводження з інформацією обмеженого доступу (Закон України «Про захист інформації в інформаційно-комунікаційних системах»)

1. Загальні відомості про інформаційну безпеку

Способи захисту інформації

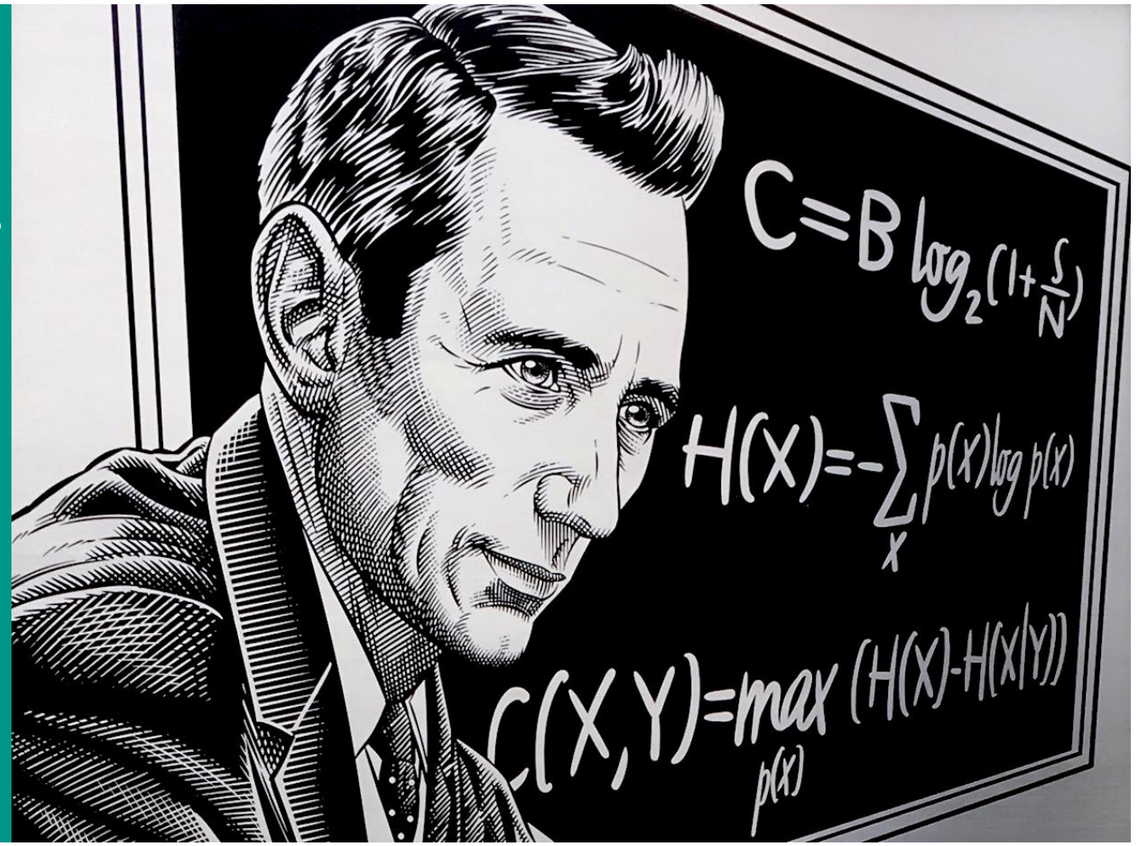
Криптографічні – вид захисту, що займається розробкою алгоритмів перетворення повідомлень, в тому числі шляхом шифрування з використанням спеціальних (ключових) даних (шифрування, хешування, цифрові підписи, протоколи автентифікації)

2. Основні поняття криптології

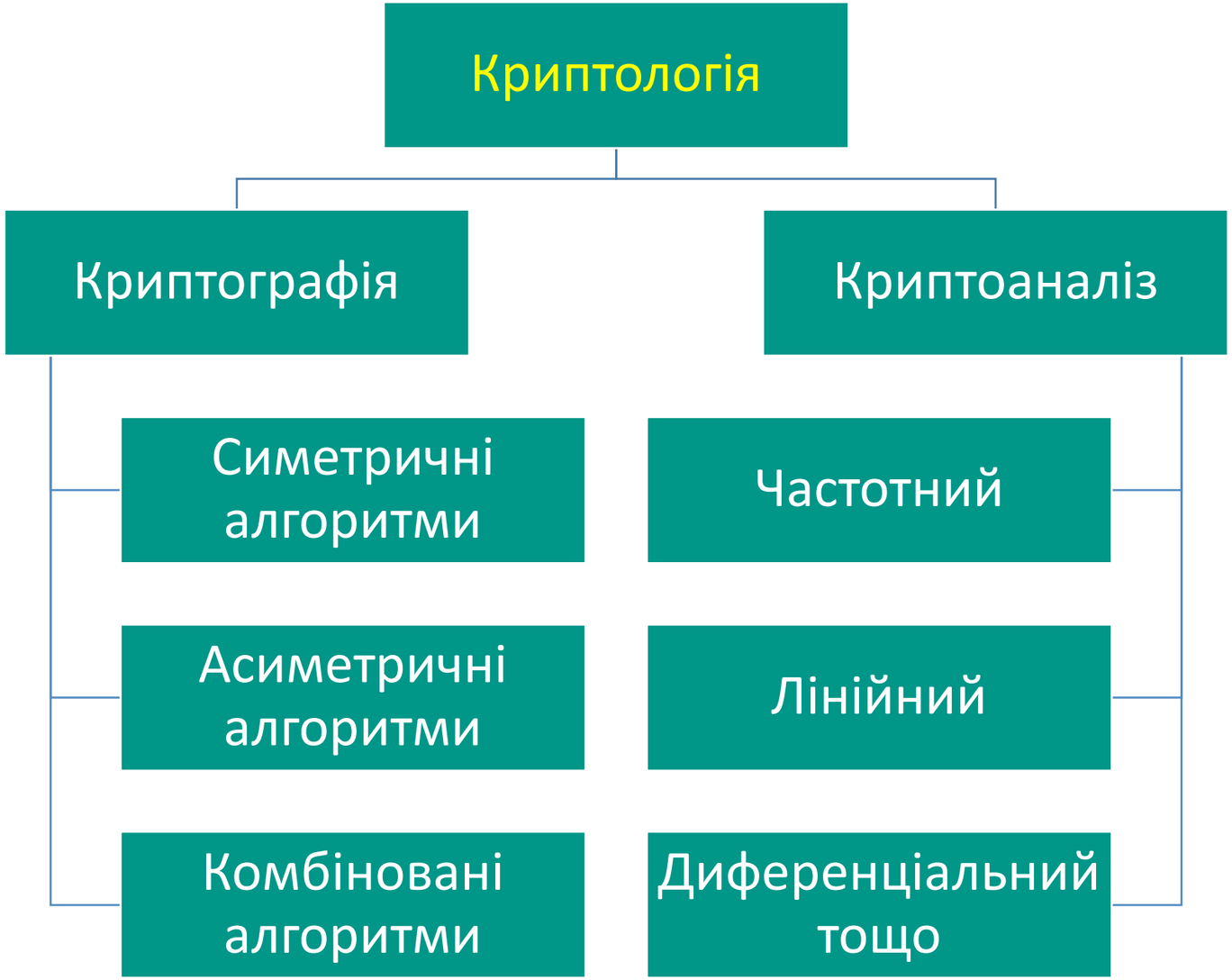
Криптологія (грецьк. «таємний» та «слово, вчення») – наука, яка вивчає методи побудови та аналізу систем захисту інформаційних ресурсів, основаних на математичних перетвореннях даних з використанням секретних параметрів

2. Основні поняття криптології

Фундамент криптології як науки у 1949 р. заклала робота американського вченого Клода Шеннона «Теорія зв’язку в секретних системах», у якій фактично вперше було представлено математичну модель шифрів



2. Основні поняття криптології



2. Основні поняття криптології

Криптографія (грецьк. «таємний» та «писання», «тайнопис») – наука про принципи, засоби та методи перетворення даних з метою приховування їх змісту, запобігання несанкціонованого використання або підробки

Криптоаналіз (грецьк. «таємний» та «аналіз») – наука про методи та способи розкриття зашифрованих повідомлень, а також про тактику та стратегію їх застосування

2. Основні поняття криптології

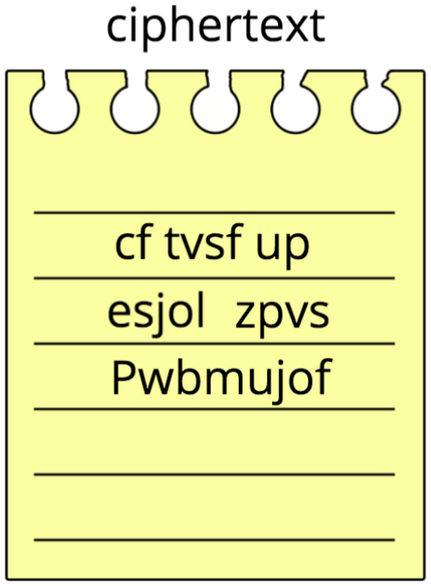
Криптографічний алгоритм – набір математичних правил та процедур, який описує такі види перетворень, як шифрування, хешування, створення та перевірка цифрових підписів тощо

Сукупність криптографічних алгоритмів, що використовуються для шифрування називають **шифром**

2. Основні поняття криптології

Відкритий текст являє собою вихідне повідомлення, що підлягає зашифруванню

Результатом зашифрування відкритого тексту є **шифротекст**, що також називають **криптотекстом** або **криптограмою**



2. Основні поняття криптології

Шифрування даних – це процес, що складається із

Зашифрування – процес перетворення відкритого тексту до виду, незрозумілого несанкціонованому користувачеві

Розшифрування (син. **дешифрування**) – процес перетворення шифрованого повідомлення до початкової інформації (відкритого тексту) за допомогою певних правил шифру та відомого ключа

2. Основні поняття криптології

Криптографічний ключ (ключ)– таємний стан деяких параметрів алгоритму криптографічного перетворення, що забезпечує вибір одного перетворення із сукупності можливих для даного алгоритму (секретний змінний елемент шифру, що застосовується для шифрування конкретного повідомлення)

2. Основні поняття криптології

Криптосистема – це система криптографічного перетворення даних, що містить у собі п’ять компонентів:

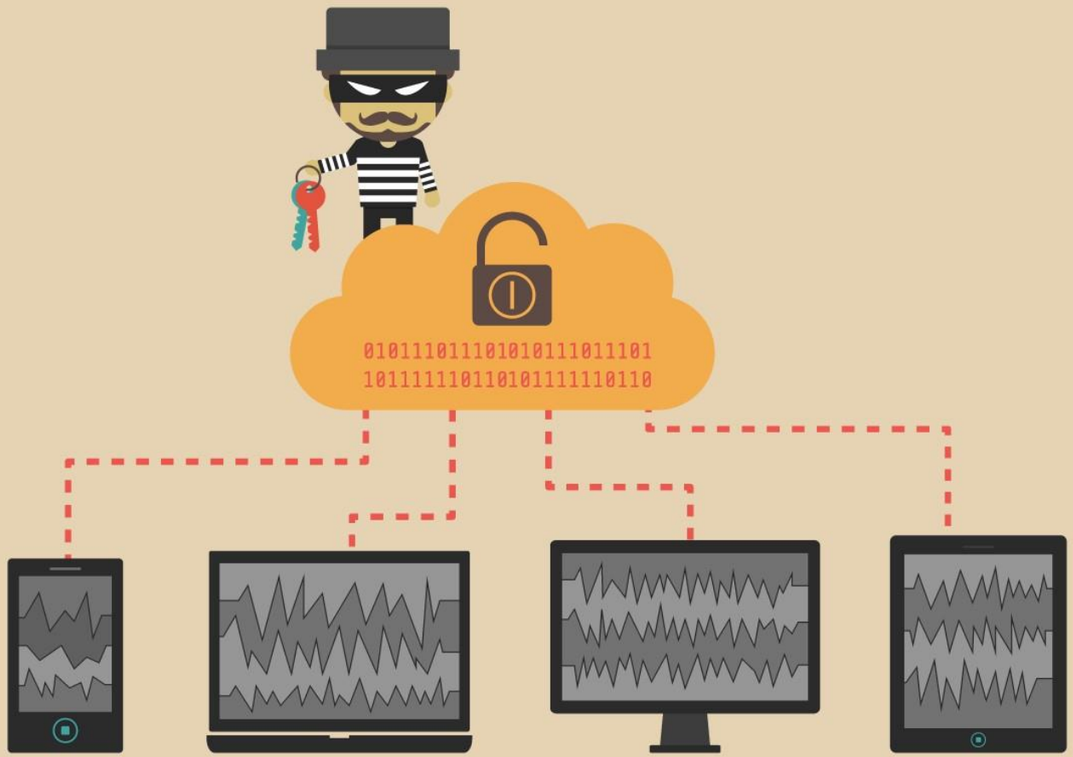
- множину відкритих текстів
- множину шифро-текстів
- множину ключів
- сімейство зашифро-вуючих перетворень
- сімейство розшифро-вуючих перетворень

2. Основні поняття криптології

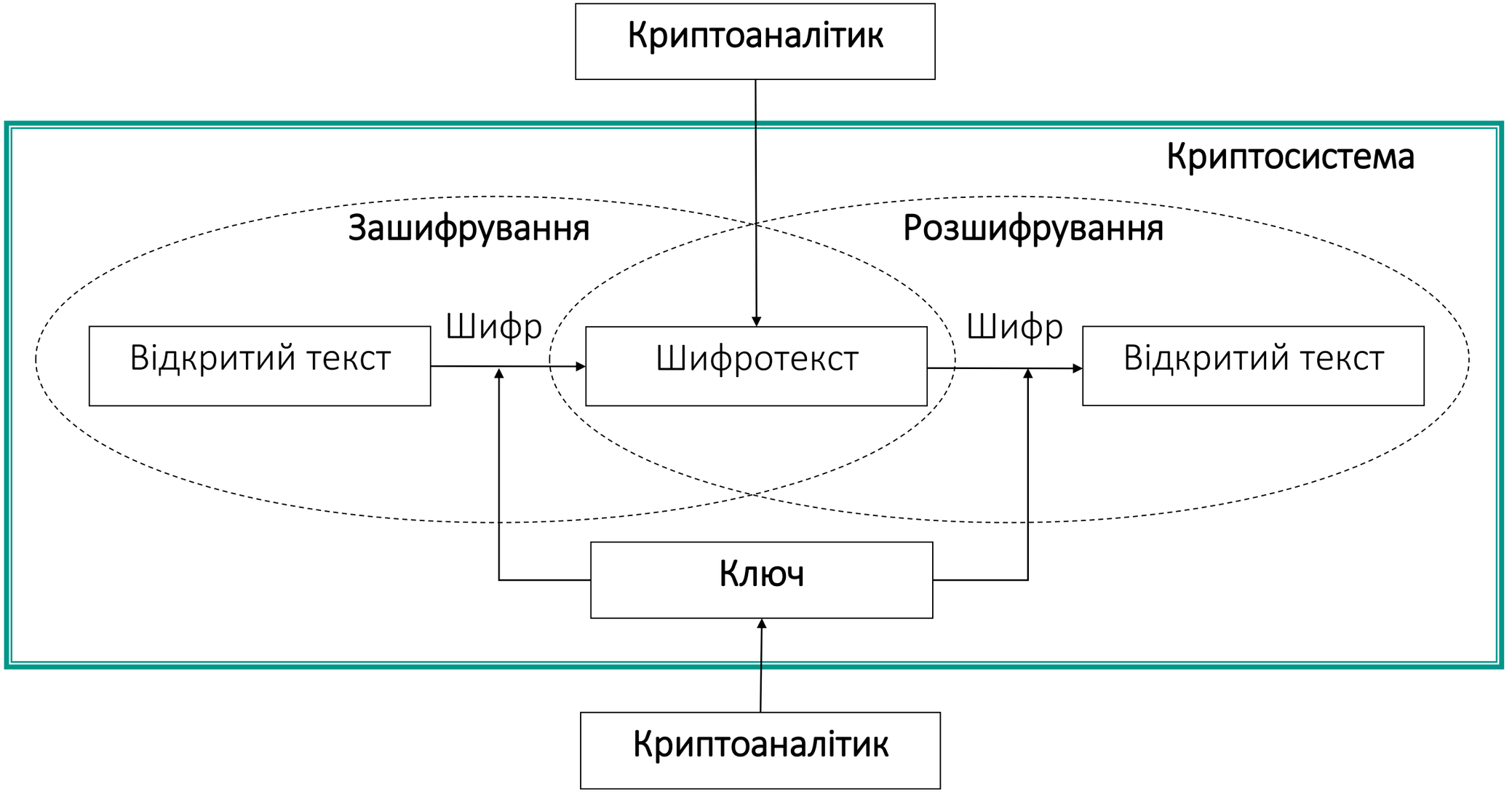
Криптостійкість – це властивість криптосистеми протидіяти атакам супротивника, спрямованим на отримання секретного ключа або відкритого повідомлення

Під **атакою** на криптосистему розуміється спроба порушення безпеки конкретної реалізації криптосистеми.

Вдалу криптоатаку називають **зламом**



2. Основні поняття криптології



2. Основні поняття криптології

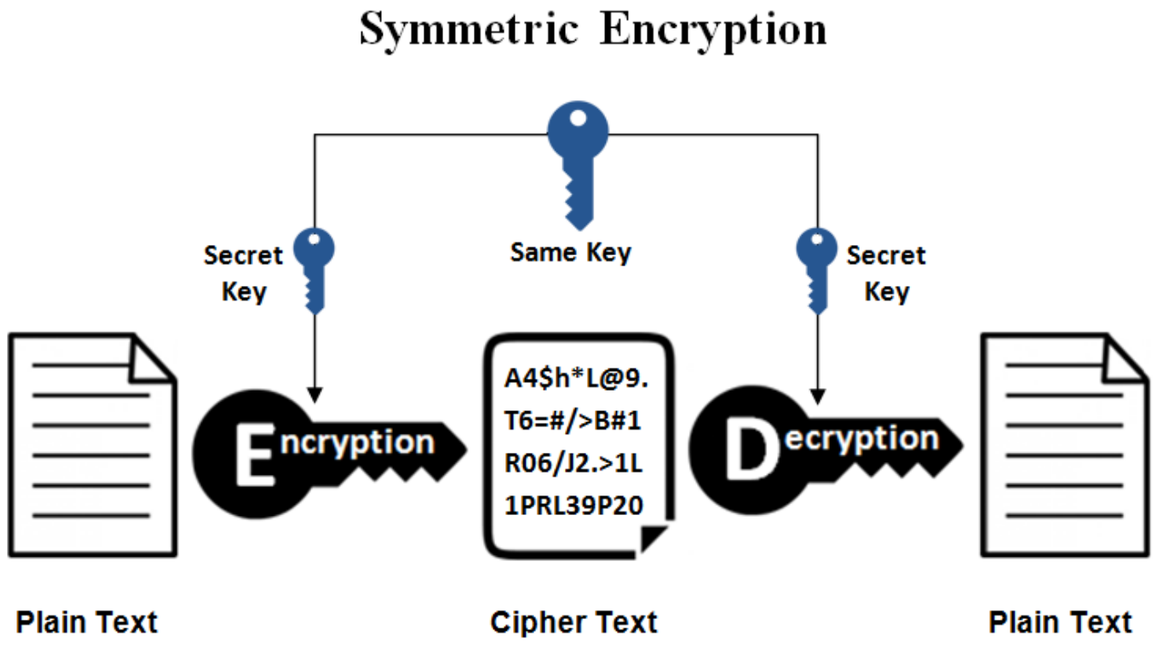
Принципи криптології

Принцип рівної міцності захисту	повідомлення мають бути **однаково міцно захищені** на **кожній ланці** передачі даних, в залежності від загроз, що виникають
Принцип доцільності захисту	проблема **співвідношення вартості** даних, витрат на їх захист та витрат на їх злам
Принцип використання ключа	без знання **ключа дешифрування** даних має бути практично **неможливим**
Принцип стійкості шифру	здатність шифру **протидіяти** різноманітним атакам на нього є його стійкістю, вона оцінюється шляхом різноманітних спроб його зламу
Принцип Керкхоффа	стійкість сучасного шифру має визначатись, **в першу чергу, ключем**
Принцип використання різноманітних шифрів	**вибір шифру** залежить **від особливостей інформації**, від її обсягу, цінності тощо

3. Класифікація шифрів

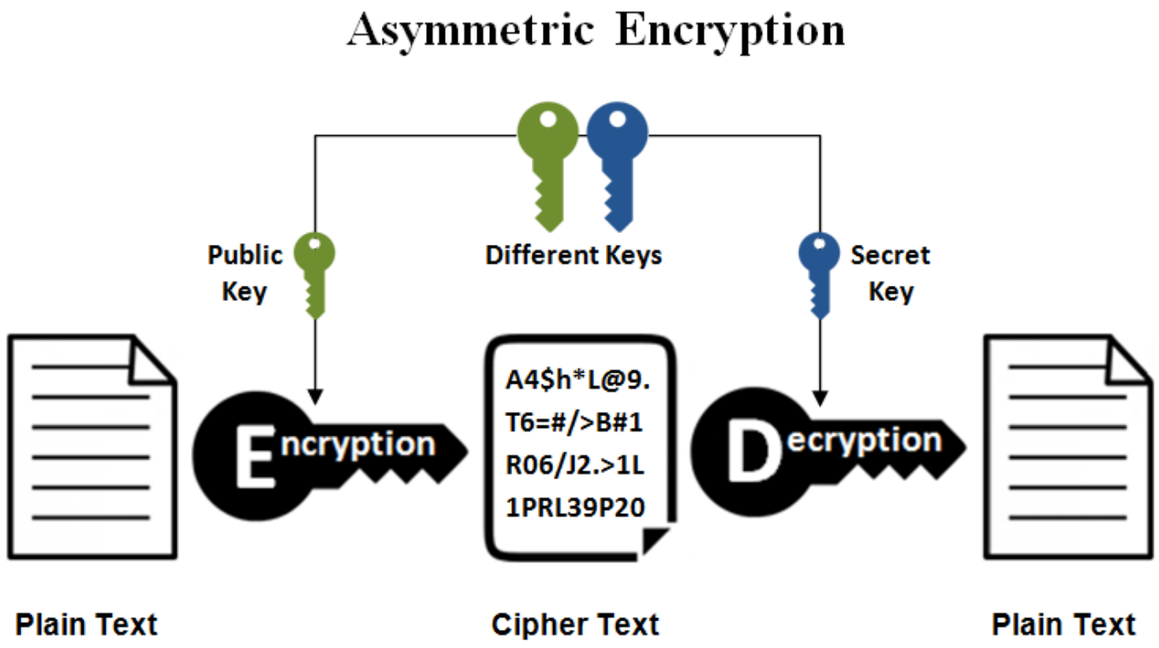
3. Класифікація шифрів

Симетричний шифр (з закритим ключем) – метод шифрування, в якому один і той самий алгоритм, а також один і той самий ключ використовується для шифрування та дешифрування повідомлень



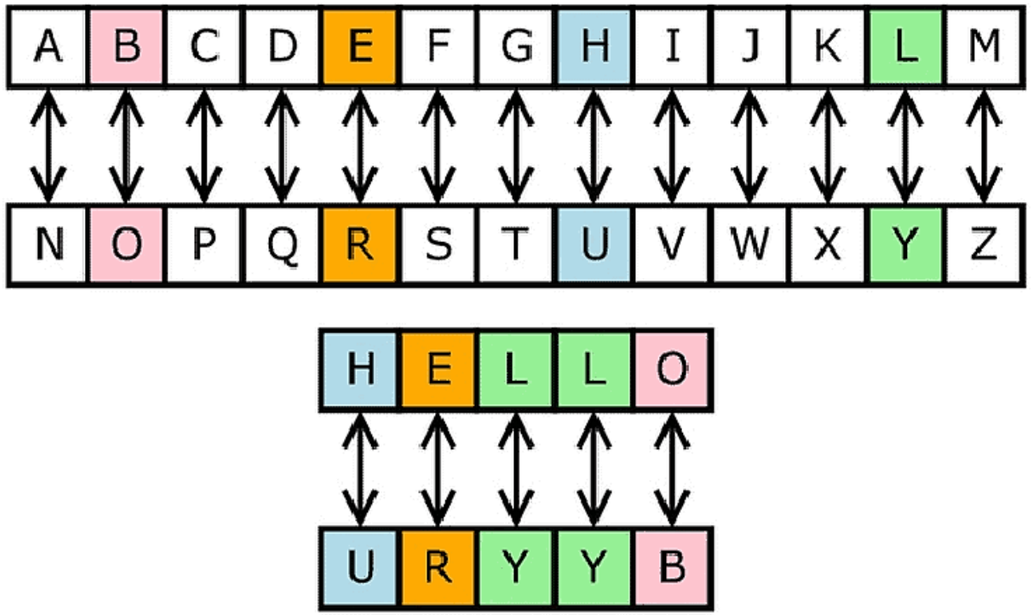
3. Класифікація шифрів

Асиметричний шифр (з відкритим ключем) – метод шифрування, в якому алгоритми шифрування та дешифрування різні, і використовуються два ключа – один для шифрування, а другий – для дешифрування повідомлень



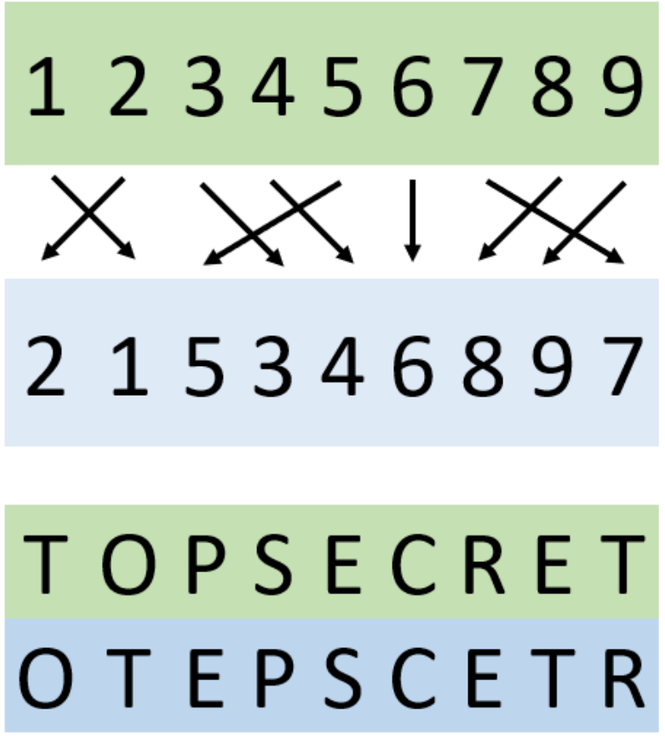
3. Класифікація шифрів

Шифр заміни (підстановки) – це шифр, у якому кожен символ відкритого тексту у шифротексті замінюється іншим символом



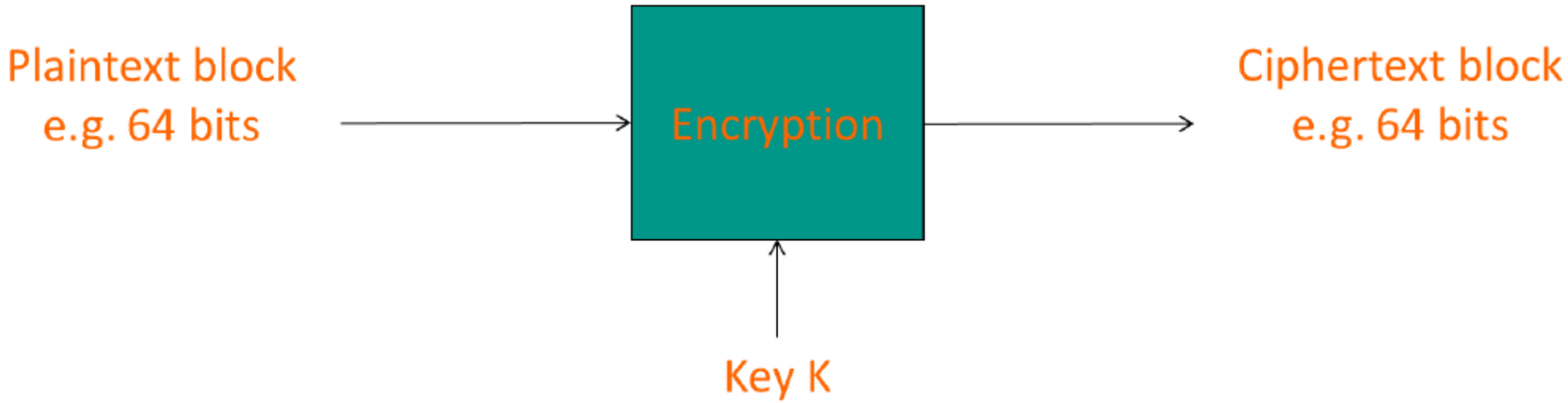
3. Класифікація шифрів

Шифр перестановки – це шифр, у якому символи повідомлення переставляються місцями безпосередньо у відкритому тексті за певним правилом, що залежить від ключа



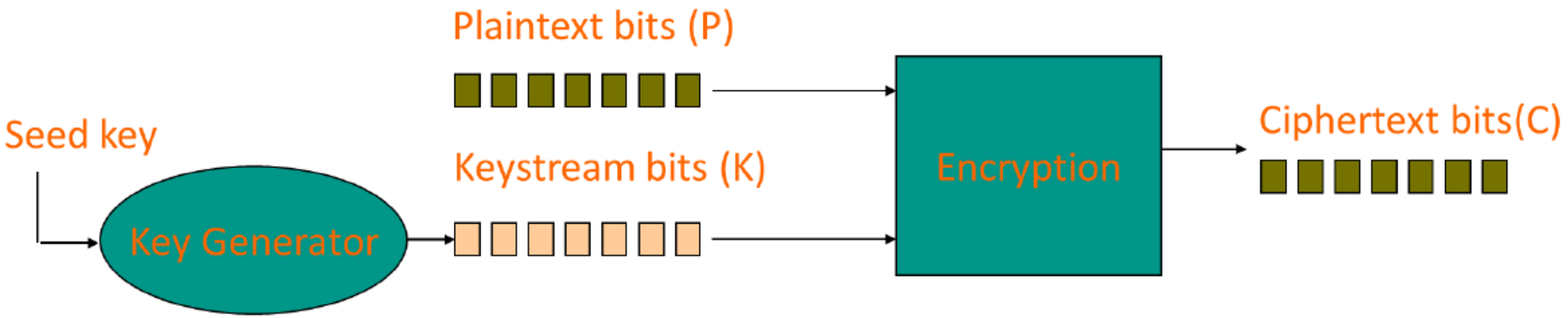
3. Класифікація шифрів

Блокові шифри здійснюють шифрування блоків фіксованої довжини, що складаються з послідовності символів відкритого тексту



3. Класифікація шифрів

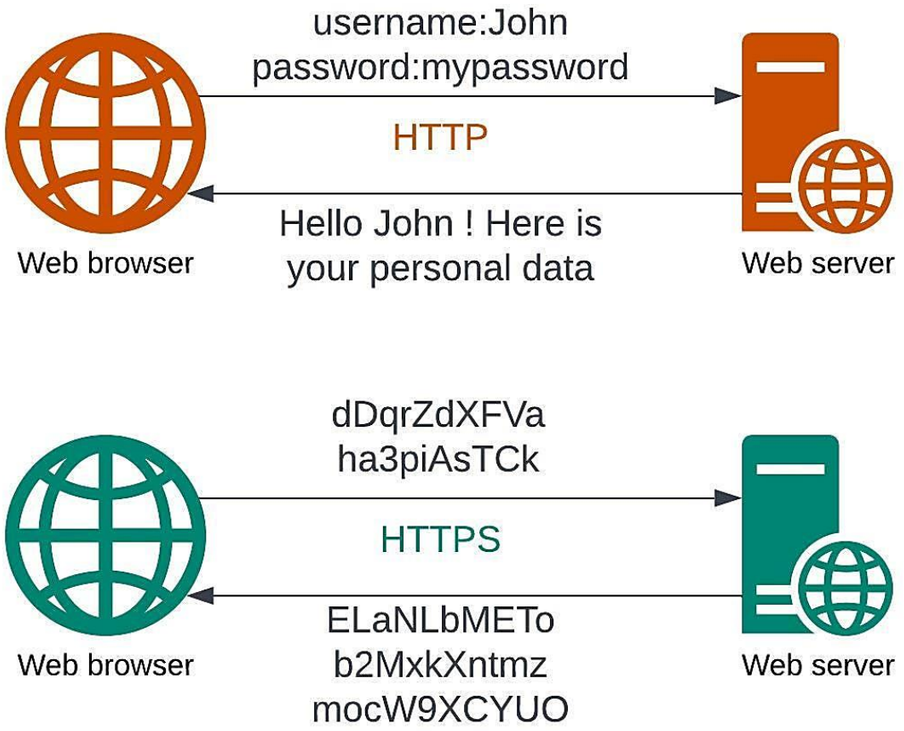
Потокові шифри здійснюють шифрування окремих символів відкритого тексту



4. Застосування криптографії у сучасному світі

Мережеві протоколи

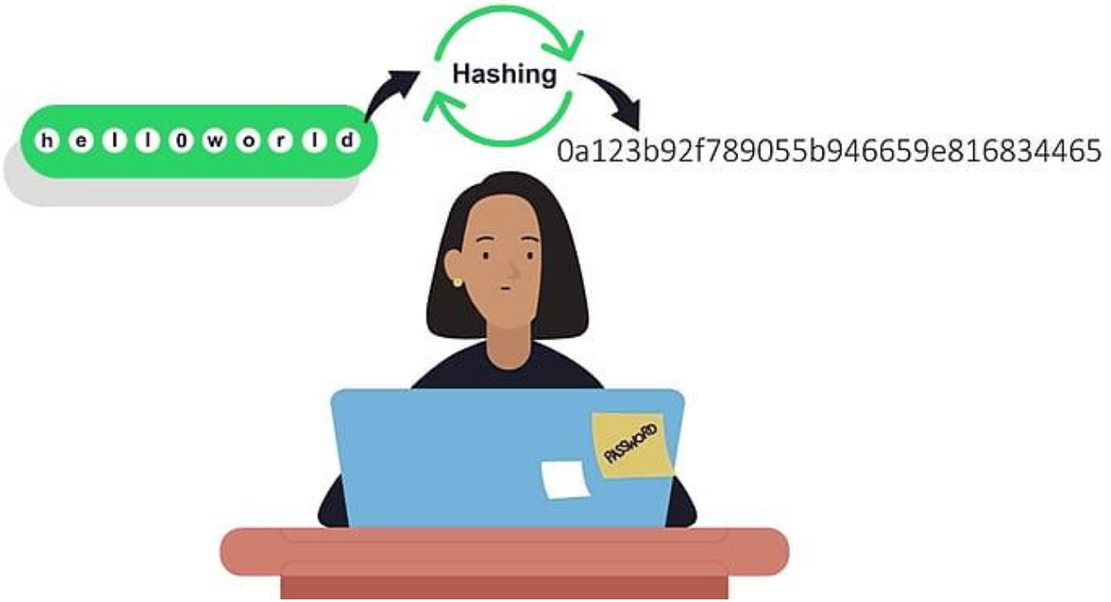
Протокол HTTPS, який використовує SSL/TLS шифрування, забезпечує захищене з'єднання між користувачем і сервером під час перегляду веб-сайтів



4. Застосування криптографії у сучасному світі

Зберігання паролів

Криптографія дозволяє безпечно зберігати паролі та інші конфіденційні дані шляхом їх хешування



4. Застосування криптографії у сучасному світі

Електронна комерція

Криптографія використовується для захисту платіжних систем, безпеки транзакцій під час онлайн-платежів, переказів коштів та доступу до банківських рахунків

4. Застосування криптографії у сучасному світі

Обмін повідомленнями

Деякі месенджери та мобільні додатки використовують криптографію для захисту конфіденційності користувачів шляхом шифрування повідомлень, фото та дзвінків

4. Застосування криптографії у сучасному світі

Блокчейн-технології

Багато блокчейн-платформ і криптовалют використовують криптографію для створення ключів і підписання транзакцій