Основи криптографії. Алгоритми з симетричним криптографічним ключем

AGENDA

- **Безпека в комп’ютерних мережах**
- **Основи криптографії**
- **Алгоритми з симетричним криптографічним ключем**
- **Плутанина і поширення (confusion and diffusion)**
- **Стандарт шифрування даних DES**
- **Покращений стандарт шифрування AES**
- **Режими шифрування**

Безпека в комп’ютерних мережах

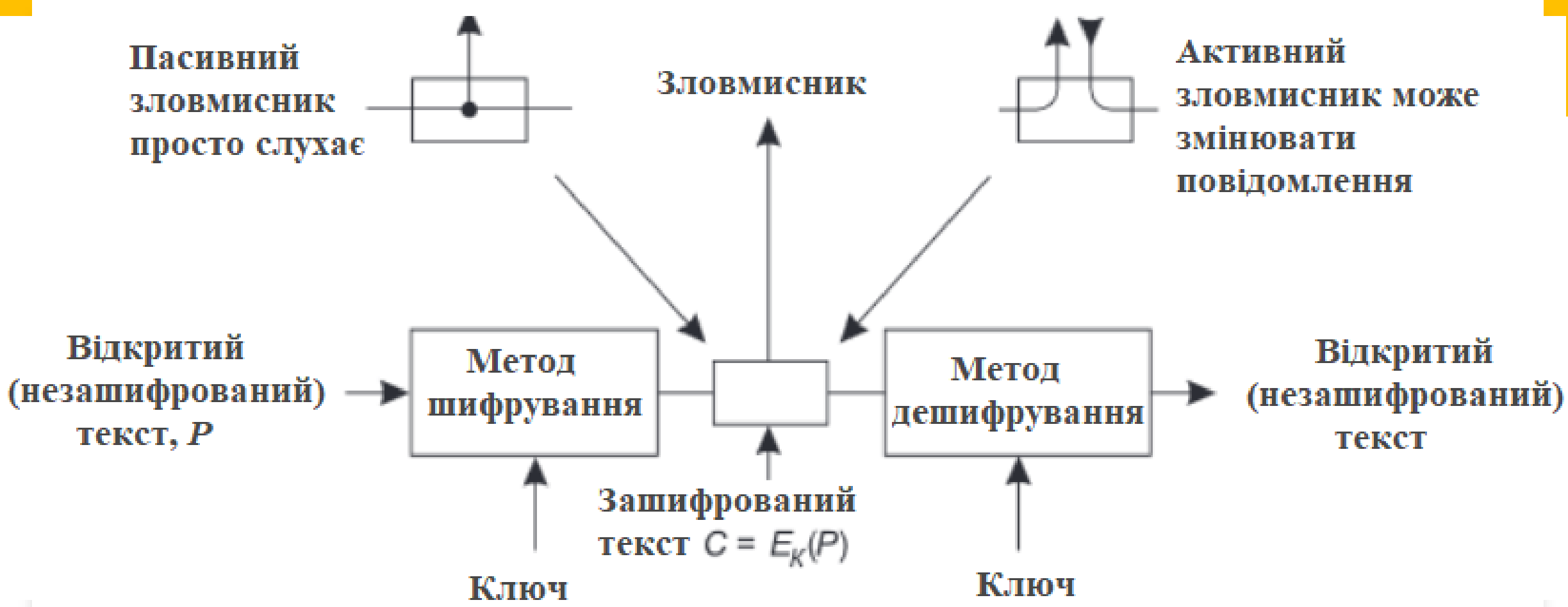
- У першому наближенні проблеми безпеки мереж можуть бути розділені на чотири пересічні області: секретність, аутентифікація, забезпечення суворого виконання зобов'язань і забезпечення цілісності.
- Секретність (конфіденційність) означає запобігання потрапляння інформації в руки неавторизованих користувачів.
- Аутентифікація дозволяє визначити, з ким ви розмовляєте, перш ніж надати співрозмовнику доступ до секретної інформації або вступити з ним в ділові відносини.

Безпека в комп’ютерних мережах

- Проблема забезпечення суворого виконання зобов'язань має справу з підписами. Як довести, що ваш клієнт дійсно надіслав електронною поштою замовлення товару за однією ціною, якщо згодом він стверджує, що ціна була іншою?
- Нарешті, контроль цілісності має справу з тим, як можна бути впевненим, що прийняте вами повідомлення не модифіковано зловмисником і не підроблено?
- На всіх рівнях, за винятком фізичного, захист інформації в мережах базується на принципах криптографії.

Основи криптографії

- Криптографія — наука про математичні методи забезпечення конфіденційності, цілісності і автентичності інформації.
- Криптографія відома з давніх часів, але тільки публікація в 1949 р статті Клода Шеннона «Теорія зв'язку в секретних системах» стала початком нової ери наукової криптології з секретними ключами. У цій блискучій роботі Шеннон пов'язав криптографію з теорією інформації.
- В контексті криптографії важливими термінами є шифр, шифрування, дешифрування.



Основи криптографії

- У криптографії шифр - це алгоритм виконання шифрування або дешифрування - це ряд чітко визначених етапів, які можна виконати як процедуру.
- Модель процесу шифрування - дешифрування показана на рис.

Основи криптографії

- Формула $C = E_K(P)$ означає, що при зашифровці відкритого тексту P за допомогою ключа K виходить зашифрований текст C. Аналогічно, формула $P = D_K(C)$ означає розшифрування зашифрованого тексту C.
- В сучасній криптографії має місце так званий принцип Керкгофа:
- **Алгоритми шифрування загальнодоступні; секретні тільки ключі.**
- Секретності алгоритму не варто надавати великого значення. Спроба зберегти алгоритм в таємниці, що у торгівлі зветься безпекою за рахунок неясності (security by obscurity), приречена на провал.

Основи криптографії

- Історично методи шифрування розділилися на дві категорії: підстановочний шифр (substitution cipher) і перестановочний шифр (transposition cipher).
- У підстановочному шифрі кожен символ або група символів замінюється іншим символом або групою символів.
- Прикладом підстановочного шифру є шифр Цезаря, в якому кожна буква відкритого тексту заміняється на ту, що віддалена від неї в алфавіті на сталу кількість позицій.
- У перестановочному шифрі змінюється послідовність символів, але не змінюють самі символи.
- Прикладом перестановочного шифру є шифр Скітала. Скітала являла собою дерев'яний циліндр, на який намотувалась шкіряна стрічка (див. зверху). Перпендикулярно стрічці писалось повідомлення, потім стрічка розмотувалась і передавалась одержувачу.

Основи криптографії

- Криптографія має два фундаментальних принципи, порушувати які не слід:
- 1. **Надлишковість: повідомлення повинні містити надлишкові (redundancy) дані.**
- Іншими словами, при розшифровці повідомлення одержувач повинен мати можливість перевірити його справжність шляхом аналізу і, можливо, виконання нескладних обчислень. Надмірність потрібна для того, щоб можна було протистояти намаганням активних зловмисників обдурити одержувача фальшивими повідомленнями, що містять сміття. Разом з тим, додавання надлишкової інформації полегшує пасивним зловмисникам завдання злому системи, так що тут є певна суперечність.

Основи криптографії

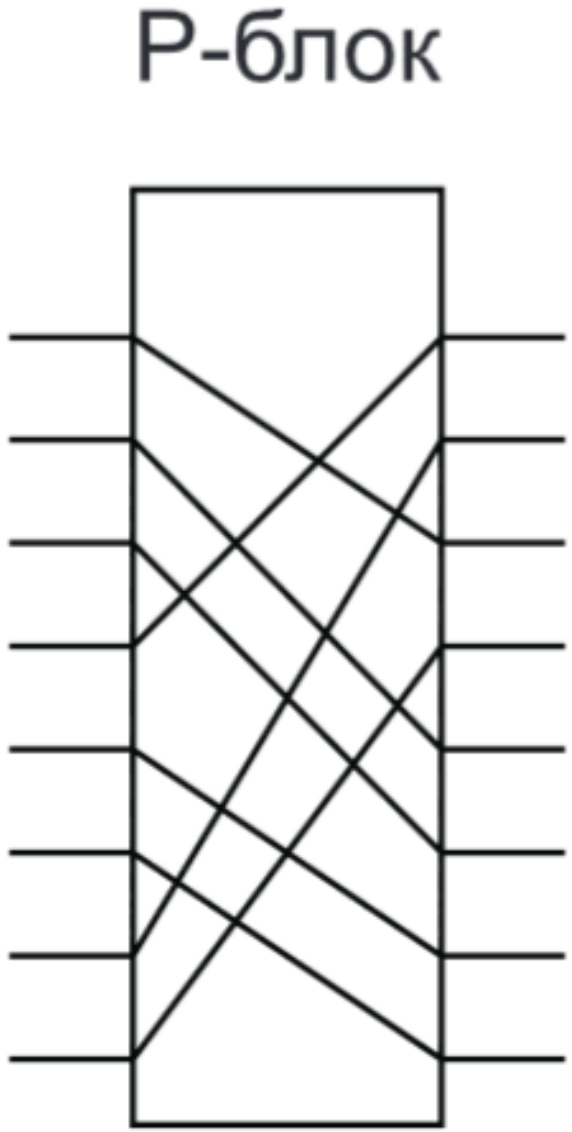
- **2. Обмежений термін придатності: необхідний спосіб боротьби з повторною відправкою повідомлень, які були відправлені раніше.**
- Цей захід спрямований на боротьбу з активними зловмисниками, що відтворюють перехоплені ними старі повідомлення. Одним з подібних заходів є включення в кожне повідомлення часової позначки (timestamp), дійсного, скажімо, тільки протягом 10 с. Одержувач може просто зберігати прийняті повідомлення протягом 10 секунд, відсіваючи дублікати. Повідомлення віком понад 10 с просто ігноруються як застарілі.

Алгоритми з симетричним криптографічним ключем

- У алгоритмі з симетричним ключем (symmetric-key algorithms) для шифрування і дешифрування повідомлень застосовується один і той же ключ.
- Зокрема, ми розглянемо блокові шифри (block ciphers), які беруть на вході n-бітові блоки відкритого тексту і перетворять їх з використанням ключа в n-бітний шифр.
- Розглянемо принципи побудови криптографічної апаратури.

Алгоритми з симетричним криптографічним ключем

- Підстановки і перестановки можуть бути реалізовані за допомогою простих електричних ланцюгів. На рис. , показано пристрій, що називається P-блоком (P-box, літера P означає permutation - перестановка) і використовується для перестановки восьми вхідних розрядів.

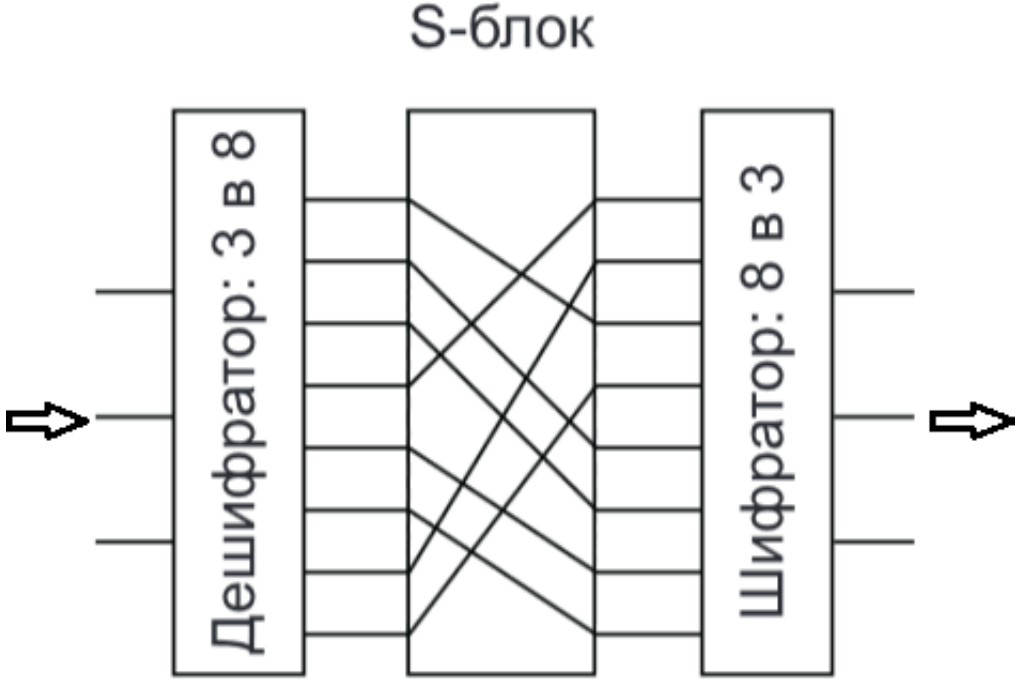


Алгоритми з симетричним криптографічним ключем

- Якщо пронумерувати вхідні біти зверху вниз (01234567), вихід цього конкретного P-блоку буде виглядати як 36071245. За допомогою відповідного внутрішнього устрою P-блоку (розпаювання проводів) можна змусити його виконувати будь-яку операцію перестановки практично зі швидкістю світла, так як ніякі обчислення в ньому не потрібні, а просто передається сигнал з входу на вихід. Таке рішення відповідає принципу Керкгофа: зломщик знає, що використовується метод перестановки бітів. Однак він не знає ключа, який полягає в порядку перестановок.

Алгоритми з симетричним криптографічним ключем

- Підстановки (тобто заміщення) виконуються S-блоками (S-box, S означає substitution - підстановка, заміна), як показано на рис. .



Алгоритми з симетричним криптографічним ключем

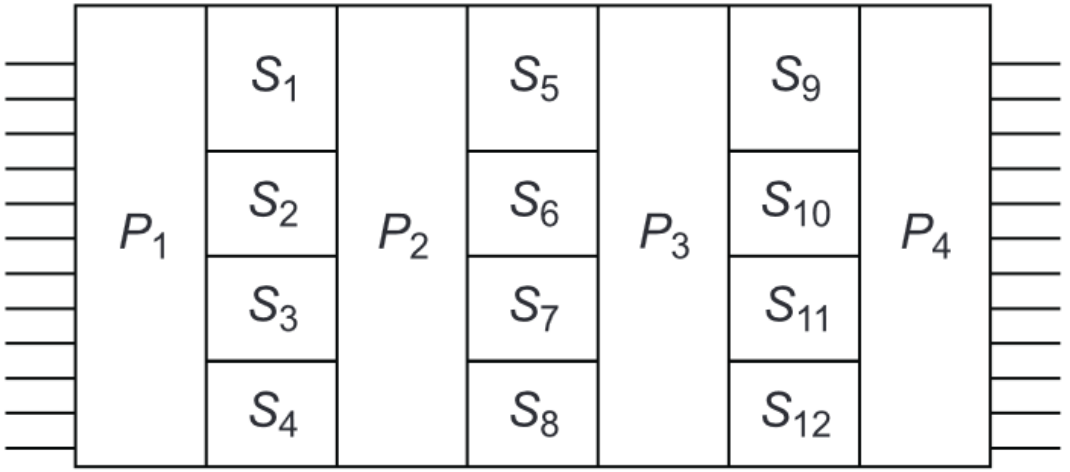
- В даному прикладі на вхід подається 3-бітний відкритий текст, а на виході з'являється 3-бітний зашифрований текст. Для кожного вхідного сигналу вибирається одна з восьми вихідних ліній декодера шляхом установки її в 1. Всі інші лінії встановлюються в 0. Потім ці вісім ліній проходять через P-блок, який представляє собою другий етап S-блоку. Третій етап виробляє зворотне кодування однієї з восьми ліній в 3-бітове двійкове число.
- Такий пристрій замінює восьмеричні числа 01234567 на 24506713 відповідно. Тобто 0 замінюється числом 2, 1 - числом 4 і т. д. Знову ж таки, при відповідному розпаюванні провідників P-блоку всередині S-блоку можна реалізувати будь-який варіант підстановки.

Алгоритми з симетричним криптографічним ключем

- Шифратори і дешифратори побудовані на напівпровідникових елементах - транзисторах, які можуть спрацьовувати за час менше 1 нс (одна чи дві вентильних затримки), а P-блок - менше 1 пс, тому апаратна реалізація S-блоку надзвичайно швидка.

Алгоритми з симетричним криптографічним ключем

- Справжня сила цих елементів стає очевидна, якщо сформувати каскад з цих пристроїв, як показано на рис. . Пристрій, який вийшов в результаті називається продукційним шифром (product cipher).



Алгоритми з симетричним криптографічним ключем

- В даному прикладі на першому етапі (P1) 12 вхідних ліній міняються місцями. На другому етапі вхід розбивається на чотири групи з трьох біт, з кожною з яких операція заміни виконується незалежно (S1 до S4). Даний метод являє собою складання більшого S-блоку з декількох менших S-блоків. Даний спосіб досить доцільний, оскільки невеликі S-блоки зручні при апаратної реалізації.
- Вихід продукційного шифру можна зробити складною функцією входу, використовуючи досить велику кількість додаткових етапів. Тому сучасні шифри, такі як DES, AES та інші, побудовані як варіанти продукційних шифрів.

Плутанина і поширення

- У криптографії, плутанина і поширення (confusion and diffusion) — це дві властивості дій стійкого шифру, які було означені Клодом Шенноном в його роботі “Теорія зв'язку в системах з секретністю”.
- Плутанина означає, що кожна двійкова цифра (біт) шифротексту повинна залежати від декількох частин ключа, затемнюючи зв'язки між ними.
  Властивість плутанини приховує зв'язок між шифротекстом і ключем.
  Ця властивість ускладнює пошук ключа з шифротексту, і якщо один біт у ключі буде змінено, це вплине на обчислення значень більшості або всіх бітів у шифротексті.

Плутанина і поширення

- Поширення означає, що зміна навіть одного біту відкритого тексту повинна спричиняти повну зміну шифротексту непередбачуваним і псевдовипадковим чином.
- Ідея поширення полягає у приховуванні зв’язку між шифротекстом та простим текстом.
- Це ускладнить завдання зловмиснику, який намагається визначити простий текст за шифротекстом.

Плутанина і поширення

- Один S- або P-блок не має особливої криптостійкості: S-блок можна розглядати як підстановочний шифр, а P-блок як перестановочний шифр. Однак, добре продуманий продукційний шифр (SP-мережа) з кількома почерговими раундами S- і P-блоків вже задовольняє властивостям плутанини і поширення.

Стандарт шифрування даних DES

- Історично першим стандартом шифрування даних для несекретних відомостей, заснованим на алгоритмах із симетричним криптографічним ключем, став DES, який прийнято урядом США у 1977 році.
- DES (Data Encryption Standard - стандарт шифрування даних) - продукційний блочний шифр широко використовувався в економіці для захисту інформації майже до 2000-х років.

Стандарт шифрування даних DES

- Відкритий текст шифрується блоками по 64 біта, в результаті чого на виході виходять 64-бітові блоки зашифрованого тексту. Алгоритм, що використовує 56-розрядний ключ, складається з 19 окремих етапів. Етапи при розшифровці просто виконуються в зворотному порядку.
- Через занадто короткий ключ, дані, зашифровані DES в наш час легко розшифровуються, тому IBM був запропонований стандарт Triple DES (потрійний DES). У ньому використовуються два 56-розрядних ключа і три етапи шифрування - Encrypt Decrypt Encrypt.

Покращений стандарт шифрування AES

- В кінці 1990-х стало зрозуміло, що навіть Triple DES уже не справляється з потребами економіки. Тому Національний інститут стандартів і технологій (NIST - National Institute of Standards and Technology) оголосив відкритий конкурс на новий криптографічний стандарт- AES (Advanced Encryption Standard - покращений стандарт шифрування). У 2001 році в результаті відбору із 15-ти серйозних кандидатів був вибраний алгоритм шифрування Rijndael (Райн-дол) бельгійських криптографів Джона Домена и Вінсента Раймена.

Покращений стандарт шифрування AES

- AES став домінуючим світовим криптографічним стандартом - він використовується у протоколах IPsec і SSL/TLS для віртуальних приватних мереж VPN; у програмах архівації 7 Zip, WinZip, RAR; у файловій системі NTFS.
- AES - це симетричний алгоритм блочного шифрування із розміром блоку 128 біт і ключами 128/192/256 біт.

Покращений стандарт шифрування AES

- Як і в DES, в AES застосовуються заміни і перестановки. І там, і там використуються декілька ітерацій, їх число залежить від розміру ключа і блоку і дорівнює 10 для 128-розрядного ключа і 128-бітних блоків; для максимального розміру ключа і блоків число ітерацій = 14.
- Однак, на відміну від DES, всі операції виконуються над цілими байтами, що дозволяє створювати ефективні реалізації як в апаратному, так і в програмному виконанні.

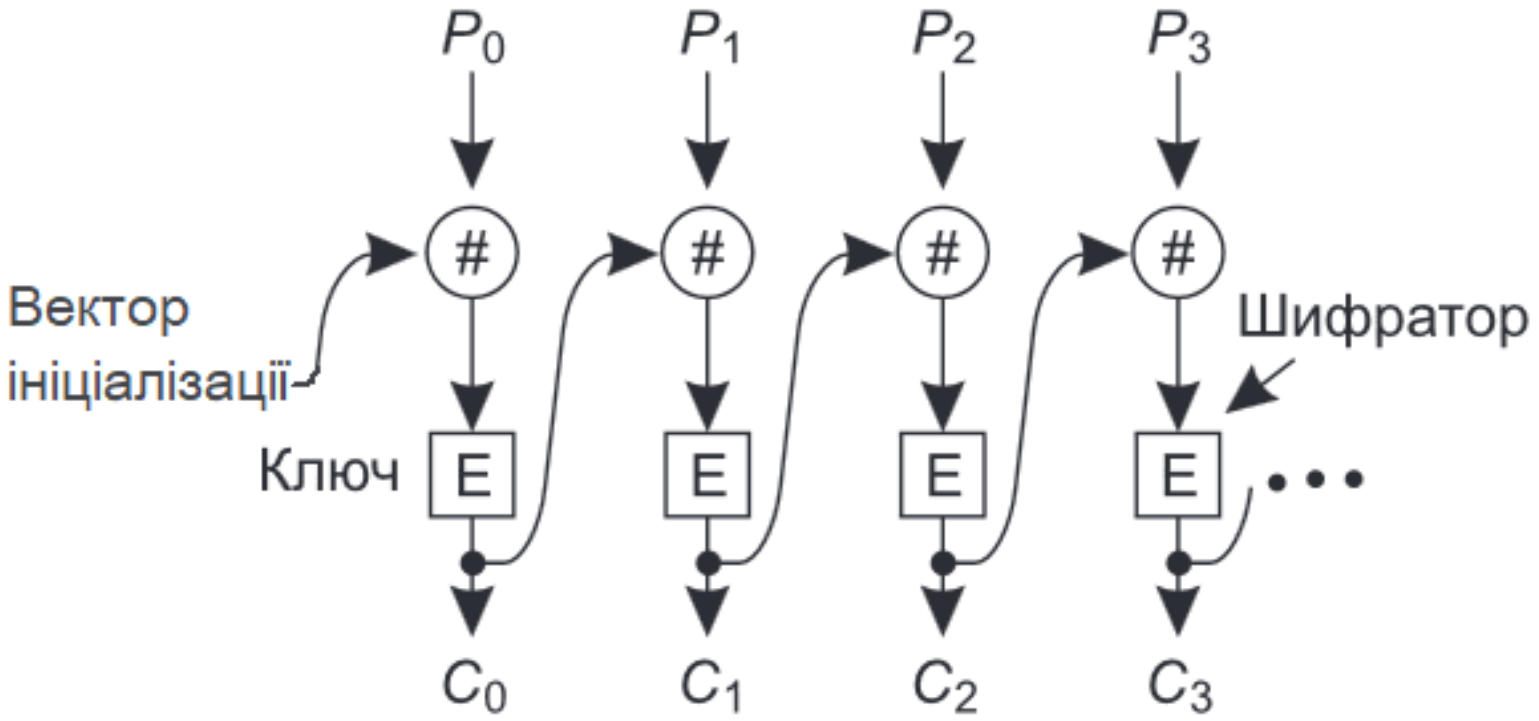
Режими шифрування

- 1. Режим електронного шифроблокнота (Electronic Code Book mode — ECB) - найпростіший режим. Це спосіб шифрування повідомлення полягає в розбитті його на окремі блоки з подальшим кодуванням цих блоків по черзі одним і тим же ключем.
- Недолік даного режиму полягає у тому, що зломщик може перехопити зашифроване повідомлення і поміняти місцями зашифровані блоки, навіть не розшифровуючи їх. При цьому сенс повідомлення зміниться. Наприклад, якщо зломщику відомо, що у другому блоці зашифрована величина премії, яку йому належить, в третьому блоці - значно більша величина премії його начальника, він просто поміняє другий і третій блок місцями.

Режими шифрування

- Режим зчеплення блоків шифру (Cipher Block Chaining mode - CBC). Щоб протистояти атакам подібного типу, всі блокові шифри можна модернізувати таким чином, щоб заміна одного блоку викликала пошкодження інших блоків відкритого тексту після їх розшифровки, перетворюючи ці блоки (починаючи з модифікованого місця) в сміття.

Режими шифрування



- У режимі , показаному на рис., кожен блок відкритого тексту P перед шифруванням складається по модулю 2 з попереднім вже зашифрованим блоком E. При цьому однаковим блокам відкритого тексту вже не відповідають однакові блоки зашифрованого тексту. Перший блок складається по модулю 2 з випадковим вектором ініціалізації, IV (Initialization Vector), переданим разом із зашифрованим текстом у вигляді відкритого тексту.

Режими шифрування

- Крім цих двох режимів, існують і інші режими шифрування, які характеризуються додатковими корисними для шифрування властивостями.

QUESTIONS

THANKS FOR YOUR ATTENTION