Лекція № 5 (НЕ 2.1, 2 год.). Симетричні криптосистеми.

План лекції:

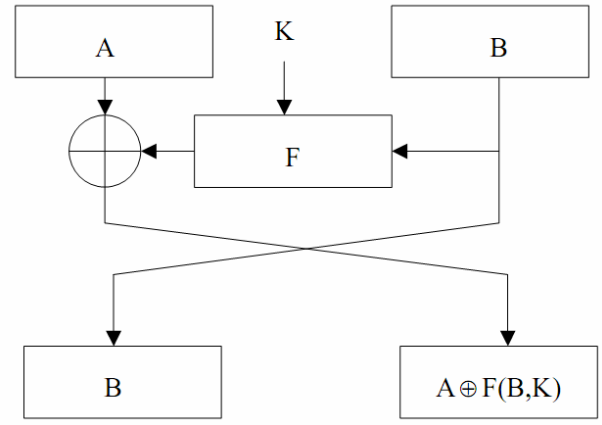
1. Петля Фейстеля, переваги і недоліки.
2. Основні властивості стандарту DES.

Зміст лекції:

1.Петля Фейстеля, її переваги та недоліки.

Одним із найпоширеніших способів задання блокових шифрів є використання так званих мереж Фейстеля. Мережа Фейстеля являє собою загальний метод перетворення довільної функції (її зазвичай називають F-функцією) в перестановку на множині блоків. Ця конструкція винайдена Хорстом Фейстелем і була використана у великій кількості шифрів, включаючи DES і ГОСТ 28147-89. F-функція являє собою основний складовий блок мережі Фейстеля і завжди вибирається нелінійною та практично в усіх випадках незворотною.

Нехай M - блок тексту, зобразимо його у вигляді двох підблоків однакової довжини M = {A,B}. Тоді один цикл (ітерацію) мережі Фейстеля визначають так:



$$M_{i+1} = B_i \| (F(B_i, k_i) \oplus A_i),$$

де $M_i = \{A_i, B_i\}$, $\|$ – операція конкатенації, а $\oplus$ – побітове виключаюче АБО.

Мережа Фейстеля складається з певної фіксованої кількості циклів, яку визначають із міркувань стійкості шифру, що його розробляють. У цьому разі в останньому циклі переставляння місцями половин блоків даних не виконують, бо це не впливає на стійкість шифру. Така структура шифрів має низку переваг , а саме:

- процедури шифрування й розшифрування збігаються, лише ключову інформацію під час розшифрування використовують у зворотному порядку;
- для розшифрування можна використовувати ті ж апаратні або програмні блоки, що й для шифрування.

Недоліком мережі Фейстеля є те, що в кожному циклі змінюється лише половина блока тексту, який опрацьовують. Це призводить до збільшення кількості циклів для досягнення бажаної стійкості. Стосовно вибору F-функції чітких рекомендацій немає, проте найчастіше ця функція, яка повністю залежить від ключа, складається з нелінійних замін, перестановок і зсувів.

Інший підхід до побудови блокових шифрів ñ використання зворотних, залежних від ключа перетворень. У цьому випадку на кожній ітерації змінюється весь блок і, відповідно, загальна кількість циклів може бути зменшена. Кожен цикл є послідовністю перетворень (так званих шарів), кожне з яких виконує свою функцію. Звичайно використовують шар нелінійної оберненої заміни, шар лінійного перемішування й один або два шари підмішування ключа. Недоліком цього підходу є те, що для процедур

шифрування й розшифрування в загальному випадку не можна використовувати одні й ті ж блоки, а це збільшує апаратні або програмні витрати на реалізацію.

2. Основні властивості стандарту DES.

Найпопулярніша сучасна схема шифрування базується на стандарті DES (Data Encryption Standard ñ стандарт шифрування даних), прийнятому в 1977 році Національним бюро стандартів (NBS) США (сьогодні називається Національним інститутом стандартів і технологій NIST). Цей стандарт отримав офіційне ім'я Federal Information Processing Standard 46. Відповідно до цього стандарту дані шифруються 64-бітовими блоками з використанням 56-бітового ключа. Багатошаровий алгоритм перетворює 64-бітові блоки тексту, які надходять на вхід у 64-бітові блоки шифрованого тексту. Цей же алгоритм із тим же ключем служить для зворотного перетворення шифрованого тексту у відкритий.

Стандарт DES завоював широку популярність, неодноразово ставши при цьому обієктом полеміки на тему його безпеки. Щоб зрозуміти суть цієї полеміки, давайте коротко розглянемо історію створення і становлення DES.

У кінці 60-х IBM почала науково-дослідний проект у галузі компíютерної криптографії, який очолив Хорст Фейстель. У результаті роботи над проектом до 1971 року був створений алгоритм під кодовою назвою LUCIFER, який продали банку Ллойда (Lloydís of London) для використання в системі управління оборотом готівкових коштів, теж розробленій IBM. Шифр LUCIFER являв собою блоковий шифр Фейстела, що оперував блоками розміром 64 біти, використовуючи ключ довжиною 128 бітів. Базуючись на багатообіцяючих результах проекту LUCIFER, IBM взяла курс на створення комерційного варіанта шифру, який, в ідеалі, можна було б розмістити в одній мікросхемі. Цей напрямок очолили Уолтер Тачман і Карл Мейер, залучивши не тільки спеціалістів з IBM, але й консультантів і технічних спеціалістів. У результаті їхніх зусиль була створена вдосконалена версія шифру LUCIFER, що мала більшу криптостійкість, але зменшений до 56 бітів ключ, щоб алгоритм міг вміститися в одну мікросхему.

У 1973 році Національне бюро стандартів оголосило конкурс на найкращий проект по створенню загальнодержавного стандарту шифрування. Компанія IBM подала на конкурс результати проекту Тачмана-Мейера. Їхній алгоритм виявився безумовно найкращим з усіх запропонованих, і в 1977 році він був затверджений як стандарт шифрування даних (DES).

Але перш ніж стати офіційним стандартом, запропонований IBM алгоритм зазнав жорстокої критики, яка не вщухає до сьогодні. Нападів зазнають, в основному, дві особливості шифру. По-перше, в початковому алгоритмі LUCIFER фірми IBM використовувались ключі довжиною 128 бітів, а в запропонованому стандарті довжина ключа зменшена до 56 бітів. Критики побоювалися (і побоюються досі), що такий розмір ключа занадто малий для того, щоб шифр міг гарантовано протистояти спробам криптоаналізу з простим перебором всіх можливих варіантів (сьогодні, з бурхливим розвитком компíютерної техніки, реалізація такої атаки стала фактом). Друге серйозне заперечення критиків спрямовано проти того факту, що внутрішня структура DES, а саме структура S-матриць, була засекреченою. Тому користувачі не могли бути впевнені в тому, що у внутрішній структурі DES немає якихось дефектів, за допомогою яких спеціалісти АНБ могли б розшифрувати повідомлення, не маючи ключа. Подальші дослідження, зокрема останні праці з різницевого криптоаналізу, дозволяють із більшою впевненістю стверджувати, що DES має досить надійну внутрішню структуру. Більше того, за ствердженнями учасників проекту з боку IBM, єдиними змінами, які були внесені в представлений ними проект стандарту, були запропоновані АНБ зміни в структурі S-матриць, метою яких було укріплення

ймовірних слабких місць алгоритму, знайдених у ході оцінки проекту.
Так чи інакше, DES побачив світ і став дуже популярним, особливо у фінансових застосуваннях. В 1994 році NIST продовжив використання DES як федерального стандарту ще на п'ять років і рекомендував його до застосування в комерційних структурах.

Опис DES

DES являє собою блоковий шифр, він шифрує дані 64-бітовими блоками.
На вхід алгоритму подається 64-бітовий блок відкритого тексту, а на виході отримується 64 біти шифрограми. DES є симетричним алгоритмом: для шифрування і розшифрування використовується однаковий алгоритм і ключ.
Довжина ключа дорівнює 56 бітам. Ключ зазвичай представляється 64-бітовим числом, але кожний восьмий біт використовується для перевірки парності й ігнорується. Біти парності є найменшими значущими бітами байтів ключа.
Ряд чисел вважаються слабкими ключами, але їх можна легко уникнути. Безпека системи повністю визначається ключем.
На найпростішому рівні алгоритм не являє собою нічого, крім комбінації двох основних методів шифрування: зміщення і дифузії. Фундаментальним блоком DES є застосування до тексту одиничної комбінації цих методів (підстановка, а за нею ñ перестановка), які залежать від ключа. Такий блок називається етапом. DES складається з 16 етапів, однакова комбінація методів застосовується до відкритого тексту 16 разів.
DES працює з 64-бітовим блоком відкритого тексту. Після початкової перестановки блок розбивається на праву й ліву половини довжиною 32 біти. Після цього виконується 16 етапів однакових дій, які називаються цикловою функцією , в яких дані об'єднуються з ключем. Після шістнадцятого етапу права і ліва половини об'єднуються й алгоритм завершується кінцевою перестановкою (оберненою по відношенню до початкової).
На кожному етапі біти ключа зсуваються, а потім із 56 бітів вибираються 48. Права половина даних збільшується до 48 бітів за допомогою перестановки з розширенням, об'єднується з допомогою XOR із 48 бітами зміщеного й переставленого ключа, проходить через 8 S-блоків, утворюючи 32 нових біти, і переставляється знову. Ці чотири операції і виконуються функцією F. Потім результат функції F об'єднується з лівою половиною з допомогою іншого XOR. У результаті цих дій з'являється нова права половина, а стара права половина стає новою лівою. Ці дії повторюються 16 разів, утворюючи 16 етапів DES.

Якщо B_i – це результат i-тої ітерації, L_i і R_i – ліва і права половини B_i, $K_i = C_i + D_i$ – 48-бітовий ключ для етапу i, а F – це функція, яка виконує усі підстановки, перестановки і XOR із ключем, то етап можна зобразити як

$$L_i = R_{i-1},$$

$$R_i = L_{i-1} \oplus F(R_{i-1}, K_i).$$

Отже, основні властивості алгоритму можна підсумувати так. DES – це симетричний блоковий алгоритм, який має такі основні параметри:

- Обробляє 64-бітний блок тексту;
- Має довжину ключа 64 біти (56+8 бітів парності);
- Кількість етапів обробки – 16.