УДК 004.896:004.451.25
І. В. ИЩУК, канд. техн. наук;
В. І. ФЕДОТОВ, канд. техн. наук, ст. наук. співробітник;
М. В. МАЛЮЖЕНКО, канд. техн. наук;
Ю. В. МЕЛЬНИК, доктор техн. наук, ст. наук. співробітник,
Державний університет телекомунікацій, Київ

СТАНДАРТ ШИФРУВАННЯ ДАНИХ DES

Розглянуто загальні питання побудови стандарту шифрування даних DES. Підвищення вимог до сучасних систем обробки, зберігання та передавання даних щодо захисту від несанкціонованого доступу зумовлює необхідність подальшої розробки криптографічних стандартів на основі DES для різних застосувань. Показано важливість стандарту DES при створенні стандартів захисту даних у системах обробки інформації, а також можливість шляхом автентифікації виявляти як випадкові, так і навмисні зміни оброблюваних даних. Визначено області застосування стандарту.

Ключові слова: криптографічний стандарт; автентифікація; несанкціонований доступ; стандарт DES.

Вступ

У зв'язку з інтенсивним розвитком технічних і програмних засобів захисту електронно-обчислювальної техніки (ЕОТ) від несанкціонованого доступу постає необхідність у розробці і регламентуванні стандартів, що охоплюють процеси шифрування, автентифікації, контролю доступу, надійності зберігання та передавання даних в електронних системах обробки інформації. За матеріалами [1; 3] розглянуто приклад реалізації стандарту шифрування даних **DES** (*Data Encruption Standart*), що є основним при створенні стандартів захисту в системах обробки інформації.

Основна частина

Стандарт DES було розроблено під керівництвом Національного бюро стандартів (НБС), Управління національної безпеки (УНБ) США і фірми IBM 1977 року, діставши підтримку федерального уряду США. Його було виконано у вигляді стандарту функціональної сумісності та покладено в основу міжнародного стандарту ISO 8373-87.

У США всі розроблені стандарти шифрування, автентифікації, контролю доступу, надійності зберігання та передавання даних з метою встановлення загального рівня захищеності і функціональної сумісності оцінювалися стосовно вимог до стандарту DES.

Сьогодні цей стандарт — найбільш широко прийнятий загальнодоступний криптоалгоритм захисту несекретних даних, основною перевагою якого є те, що єдиний передбачуваний спосіб розв'язання алгоритму пов'язаний з повним перебором ключів до знаходження вірного. Саме на такий метод розкриття і розраховували його розробники, що і визначило фактичний рівень захисту стандарту.

Слід зазначити, що існує і вітчизняний стандарт шифрування даних ГОСТ 28147-89 для систем обробки інформації в мережах ЕОМ, окремих обчислювальних комплексів і ЕОМ [2]. Він включає в себе такі алгоритми шифрування (розшифрування) даних: режим простої заміни, режим гамування, режим гамування зі зворотним зв'язком і режим вироблення імітовставки.

Стандарт шифрування даних ГОСТ 28147-89 (256-бітовий ключ, 32 циклу шифрування) порівняно з алгоритмом DES (56-бітовий ключ і 16-циклів шифрування) має більш високу криптостійкість завдяки довшому ключу і великій кількості циклів шифрування.

Переваги ГОСТ 28147-89:

- можливість довільної зміни блока підстановки, що фактично є додатковим 256-бітовим ключем;
- захист від нав'язування помилкових даних (вироблення імітовставки) і однаковий цикл шифрування в усіх алгоритмах ГОСТу.

Структура алгоритму шифрування даних стандарту DES базується на наборі з восьми постійних таблиць підстановок або S-блоків, які використовуються під час шифрування і розшифрування. Критерії побудови таблиць не є загальнодоступними.

Стандарт шифрування даних реалізується як апаратними, так і програмними засобами. Після розробки DES, як і будь-яка практична система захисту, оцінювався за ступенем захищеності, витрат і зручності застосування його за призначенням.

Дослідження DES показали, що ефективна довжина ключа становить 56 біт, а кількість ключів, які слід перевірити, $7{,}6 \times 1016$.

При цьому стверджувалося, що довжина ключа є критичним параметром максимальної стійкості, забезпечується запропонованим стандартом.

Зростання вимог до сучасних систем обробки, зберігання та передавання даних щодо захисту від несанкціонованого доступу зумовлює потребу у подальшій розробці криптографічних стандартів на основі DES для різних застосувань.

Сьогодні в світі розроблено необов'язкові стандарти, що стосуються фінансових питань, захисту

технічних засобів обчислювальної техніки та оргтехніки, захисту систем зв'язку, стандарти загального призначення. Основою розробки таких стандартів є опубліковані НБС стандарти шифрування даних, керівні документи з реалізації і використання алгоритму DES, стандарти стосовно вибору режимів алгоритму DES і автентифікації даних ЕОМ.

Окрім того, НБС розробило набір спеціальних тестів перевірки апаратної частини пристроїв, що реалізують алгоритм DES. Існують офіційні вимоги до апаратного виконання цих пристроїв. Відповідно до цих вимог обов'язковим є корпусне виконання пристрою, що реалізує алгоритм, обладнання його засобами контролю фізичного доступу (такими, як блокування і сигналізація). Пристрій має підлягати частим перевіркам на правильне функціонування, аби його відмови не створювали небезпеки для конфіденційних даних.

Алгоритм DES — це основний елемент будь-якої з розроблених на його основі системи захисту даних. Принцип його функціонування полягає в тому, що за допомогою однієї з перетворювальних функцій алгоритму вхідна відкрита інформація перетворюється у вихідну закриту інформацію для вибраного конкретного ключа. При відомому ключі існує можливість обчислення і перетворювальної функції та її оберненої величини, але без ключа практично неможливо встановити, яка функція використовувалася, навіть якщо є кілька примірників відкритих і закритих даних.

Алгоритм DES забезпечує простий засіб моделювання всього сімейства перетворювальних функцій і може бути використаний для загального і спеціального застосування.

Для задач шифрування даних передбачено чотири робочих режимів: **ECB** (*Electronic Codebooc*) — електронна кодова книга. Цей режим переважно використовується для шифрування ключів (рис. 1).

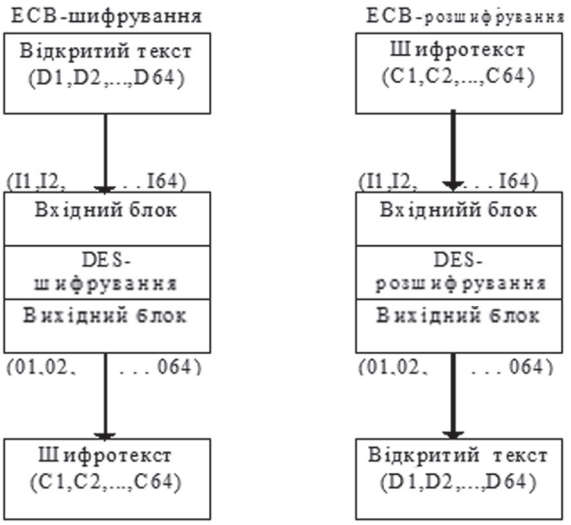

Рис. 1. Режим електронної кодової книги

CFB (*Cipher Feedback*) — зворотний зв'язок за шифротекстом. Цей режим використовується для шифрування окремих символів і автентифікації даних (рис. 2).

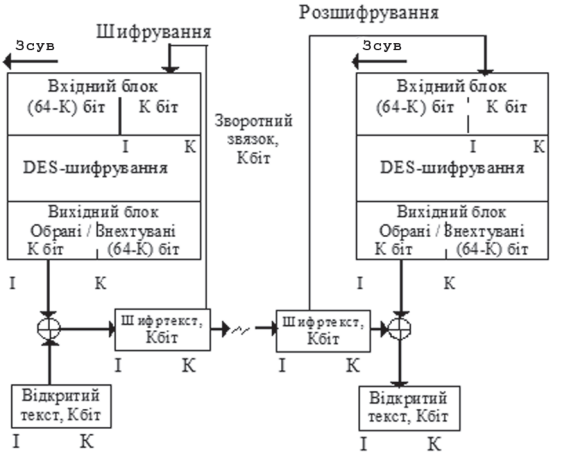

Рис. 2. Режим зворотного зв'язку за шифротекстом (CFB) блоков на К разрядів. Вхідний блок на початку містить вектор ініціалізації (IV), вирівняний по правому краю

CBC (*Cipher Blok Chaining*) — зчеплення блоків шифру, який використовується для автентифікації даних (рис. 3).

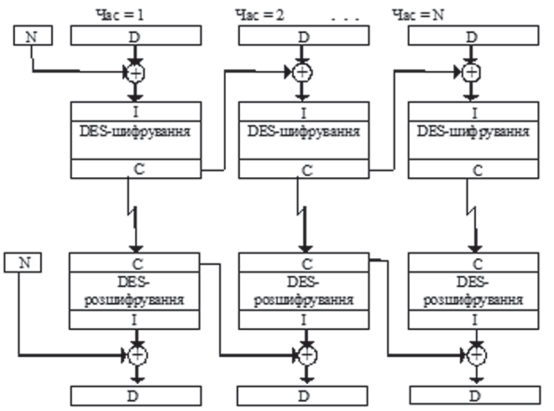

Рис. 3. Режим зчеплення блоків шифру (CBC): D — блок даних J; IV — вектор ініціалізації; I — вхідний блок шифрування J; ⊕ — вимикаюче АБО; C — блок шифру J

OFB (*Output Feedback*) — зворотний зв'язок по виходу. Цей режим використовується для шифрування в супутникових системах зв'язку (рис. 4).

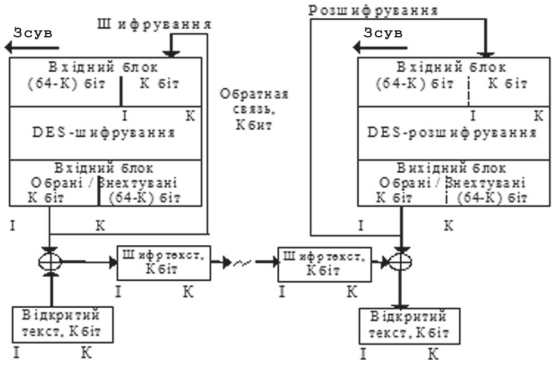

Рис. 4. Режим зворотного зв'язку по виходу (OFB) блоків на К разрядів. Вхідний блок на початку містить вектор ініциализації (IV), вирівняний по правому краю

Зазначені робочі режими дозволяють використовувати алгоритм DES для інтерактивного шифрування при обміні даними між мережними ЕОМ, шифрування криптографічних ключів у практиці автоматизованого їх поширення, шифрування файлів, поштових кореспонденцій, даних, переданих із супутників, і для інших практичних завдань.

Висновки

При автентифікації даних за допомогою алгоритму DES існує можливість утворити криптографічну контрольну суму, яка дозволить захистити дані як від випадкових, так і від навмисних, але несанкціонованих змін. Суть такого алгоритму полягає в тому, що дані зашифровуються в режимі зворотного зв'язку за шифротекстом або в режимі зчеплення блоків шифру, формуючи остаточний блок шифру, який є функцією всіх розрядів відкритого тексту.

Дані, що містять відкритий текст, можуть бути передані за допомогою обчисленого блока шифру, що слугує криптографічною контрольною сумою. Ця властивість алгоритму шифрування даних DES дає змогу через автентифікацію виявляти як випадкові, так і навмисні зміни оброблюваних даних.

Алгоритм автентифікації можна застосовувати як до відкритого, так і до зашифрованого тексту. Можливі спеціальні застосування алгоритму DES з метою забезпечення зберігання даних в ЕОМ, реалізації електронної системи платежів, електронного обміну інформацією та ін.

Сьогодні алгоритми шифрування даних широко використовуються як державними, так і комерційними організаціями для розв'язання різноманітних практичних завдань.

Список використаної літератури

1. ***Управління*** *телекомунікаціями із застосуванням новітніх технологій: підручник для ВНЗ / [В. Г. Кривуца, В. К. Стеклов, Л. Н. Беркман, Б. Я. Костік, В. Ф. Олійник, С. М. Скляренко та ін.]. Київ, 2007. 384 с.*

2. ***Хлапонін Ю. І.*** *Управління інформаційною безпекою на основі інтелектуальних технологій // Technology audit and production reserves (Технологический аудит и резервы производства) 2014. № 6/4(20). С. 47–50.*

3. ***Каллан Р.*** *Основные концепции нейронных сетей. Москва, 2003. 288 с.*

4. ***Смид М. Э., Бранстед Д. К.*** *Стандарт шифрования данных: Прошлое и будущее // ТИИЭР. 1988. Т. 76, №5. С. 43–54.*

5. ***ГОСТ 28147-89.*** *Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.*

6. ***Защита*** *информации в персональных ЭВМ / А. В. Спесивцев и др. Москва, 1993. 192 с.*

Рецензент: доктор техн. наук, професор **С. В. Козелков**, Державний університет телекомунікацій, Київ.

И. В. Ищук, В. И. Федотов, М. В. Малюженко, Ю. В. Мельник

СТАНДАРТ ШИФРОВАНИЯ ДАННЫХ DES

Рассмотрены общие вопросы построения стандарта шифрования данных DES. Повышение требований к современным системам обработки, хранения и передачи данных по защите от несанкционированного доступа обуславливает необходимость дальнейшей разработки криптографических стандартов на основе DES для различных применений. Показана роль стандарта DES при создании стандартов защиты данных в системах обработки информации, а также возможность путем аутентификации обнаруживать как случайные, так и преднамеренные изменения обрабатываемых данных. Определены области применения стандарта.

Ключевые слова: криптографичный стандарт; аутентификация; несанкционированный доступ; стандарт DES.

I. Ischuk, V. Fedotov, M. Maliuzhenko, Yu. Melnyk

STANDARD OF DESCRIPTION DATA DES

The article discusses the general issues of building a DES data encryption standard. Increasing requirements for modern data processing, storage and transmission systems for protection against unauthorized access necessitates further development of DES-based cryptographic standards for various applications. The role of the DES standard in creating data protection standards in information processing systems is shown. Ability to authenticate to detect both random and deliberate changes in the processed data. Defined the scope of the standard.

Keywords: cryptographic standards; authenticate; unauthorized access; standard DES.