

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВІННИЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
ТА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ

Контрольна робота
з дисципліни «Основи захисту інформації»

Виконав
студент групи КС-05
заочного відділення
Максим Вуєць

Перевірив
Юрій Євгенійович Яремчук

2009

Зміст

1	Шифри заміни	2
2	Шифри перестановки	5
3	Гамування	8
4	Стандарт шифрування даних DES	13
	Література	33

1 Шифри заміни

Теоретичні відомості

Заміна (підстановка) — це метод шифрування, при якому кожен знак вихідного тексту взаємнооднозначно замінюється шифропозначенням — одним, або декількома знаками деякого набору символів (алфавіту). Шифр однобуквеної простої заміни — один з найдавніших шифрів. Шифропозначення для нього застосовувались різні — від букв алфавіту до фігурок «танцюючих чоловічків». У найпростішому вигляді даний шифр полягає в тому, що буква переходить у букву, а вхідний і вихідний алфавіти збігаються як множини, тобто з точністю до перестановки. Для зашифрування чергової букви відкритого тексту визначається її номер у вхідному алфавіті і на відповідне місце формовного шифртексту поміщається буква з тим же номером, але вже з вихідного алфавіту.

Створення ключа

Вихідним алфавітом є малі літери українського алфавіту та дефіс:

а	б	в	г	г	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	-
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

Для побудови ключа скористаємось процедурою рандомізації, тобто перемішаємо вихідний алфавіт у випадковому порядку. Отримуємо такий ключ:

б	л	з	а	п	у	х	с	я	н	к	є	г	і	и	ю	ц	ч	є	й	г	р	ї	в	м	ф	щ	ж	о	ш	-	т	д	ь
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

Шифрування

Маємо наступний текст, який необхідно зашифрувати (відкрите повідомлення):

є-люди-які-беруть-у-руки-ціпок-коли-в-них-кульгають-докази

Створюємо таблицю зашифрування: зіставляємо вихідний символ алфавіту відповідному символу ключа.

а	б	в	г	г	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	-
б	л	з	а	п	у	х	с	я	н	к	є	г	і	и	ю	ц	ч	є	й	г	р	ї	в	м	ф	щ	ж	о	ш	-	т	д	ь

Використовуючи отриману таблицю зашифруємо відкрите повідомлення. Перший символ тексту «є» відповідно до таблиці кодується символом «с». Аналогічно, другий символ «-» — «ъ» і т. д. В результаті отримуємо наступне зашифроване повідомлення:

сьютукьдиеьлхгві-ъвъгвикъщейеиъиеюкьзьчкфъивю-абті-ъуеибнк

Дешифрування

Аналогічно таблиці зашифрування створюємо обернену таблицю розшифрування:

а	б	в	г	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ю	я	-	
г	а	у	р	ї	я	і	о	ч	в	к	й	т	п	и	б	ф	з	ш	г	с	є	ю	д	х	е	м	н	щ	ц	-	л	ж	ь

За допомогою цієї таблиці розшифруємо попередньо отримане повідомлення: знаходимо відповідності зашифрованих символів до відкритих. Так перший символ «с» розшифровується як «є». Другий «ъ» — «-». Після розшифрування усіх символів отримуємо:

є-люди-які-беруть-у-руки-ціпок-коли-в-них-кульгають-докази

Розшифроване повідомлення еквівалентне вихідному відкритому повідомленню. Це свідчить про правильність виконання процесів шифрування та дешифрування.

Висновки

Шифри заміни є одними із найдавніших і найслабкіших: у шифрованому тексті зберігаються усі частотні характеристики відкритого тексту, усі сполучення і повторення. Приклади дешифрування є навіть у художній літературі. Процедури шифрування та дешифрування є простими, тому можуть навіть виконуватись без застосування обчислювальної техніки.

Контрольні запитання

1. У чому полягає основна суть шифрів заміни?

Суть шифрів заміни полягає в заміні букв вихідного тексту на якісь інші букви за певною схемою, наприклад циклічний зсув алфавіту.

Тобто буква переходить у букву, а вхідний і вихідний алфавіти збігаються як множини. Для зашифрування чергової букви відкритого тексту визначається її номер у вхідному алфавіті і на відповідне місце формовного шифртексту поміщається буква з тим же номером, але вже з вихідного алфавіту.

2. *Які відмінності між рівнозначним і різнозначними шифрами заміни? Порівняйте їх за складністю і криптографічною якістю.*

У рівнозначних шрифтах всі букви кодуються однозначними числами, наприклад двозначними і весь код буде складатись з двозначних чисел.

У різнозначних шрифтах букви можуть кодуватись різнозначними числами, однозначними чи двозначними, але це не підвищує складність такого шифру в порівнянні з рівнозначним, оскільки двозначні шифропозначення починаються з цифр, які не є окремими шифропозначеннями.

Тобто криптографічна якість цих шрифтів однакова.

3. *Які відмітні риси кодів, порівняйте їх із шифрами простої і парної заміни?*

Особливістю кодів є те, що вони оперують не з довільними комбінаціями символів, а зі словами, складами і фразами. У найпростішому випадку код являє собою список, у якому кожній відкритій величині (слову, фразі) відповідає кодова група: комбінація символів, яка замінює відповідну величину під час зашифрування. Значність кодових груп постійна. Зазвичай до складу коду входять також деякі допоміжні величини — цифри, розділові знаки.

Коди мають більшу криптографічну якість ніж шифри заміни але водночас вони менш зручні у використанні, тому що потребують певного «словника» для дешифрування повідомлення.

Шифр простої заміни оперує заміною символів в той час як в кодї замінюються цілі слова і словосполучення, що призводить до ускладнення процесу злому коду за допомогою частотного аналізу.

Також до недоліків кодів відноситься складність автоматичного шифрування в порівнянні з шифрами, тому коди частіше використовують як засіб ручного шифрування.

4. *Поясніть, наскільки криптографічно стійкими є шифри заміни?*

У шифрованому тексті зберігаються всі частотні характеристики відкритого тексту, усі сполучення і повторення. Цей шифр легко розкрити за допомогою частотного аналізу, так як він не міняє частоти використання символів в тексті. Тобто шифр заміни має дуже малу криптографічну стійкість і розшифрувати його за допомогою комп'ютера дуже легко.

5. *Якими могли б бути способи спрощення побудови ключів шифрів простої заміни? Чи знижують ці особливості побудови ключів загальну стійкість застосованого шифру?*

Для ручного шифрування важливим є легкість запам'ятовування ключа і простота самого процесу дешифрування. Наприклад використання гасел може значно полегшити запам'ятовування ключа.

Спрощення ключа шифру зазвичай призводить до зменшення стійкості самого шифру, щоб запобігти цьому можна використовувати більш складні чи просто не звичні алгоритми шифрування, наприклад «книжковий шифр» або «шифр пропорційної заміни» які при не значному ускладненні алгоритму шифрування і ключів дають набагато більшу якість в порівнянні з звичайним шифром заміни.

2 Шифри перестановки

Теоретичні відомості

Шифри типу перестановки застосовувались ще у античні часи. Відмінність цього типу шифру від шифрів заміни полягає в тому, що під час зашифрування буква a_i відкритого тексту переходить не у фіксований знак алфавіту, а в іншу букву того ж відкритого тексту, скажемо a_j , у результаті чого букви розташовуються на нових місцях, тобто переставляються. Ключем для даного шифру також служить таблиця заміни, тільки не букв алфавіту, а їхніх індексів (номерів місць) у тексті, який підлягає зашифруванню. У загальному випадку розмір таблиці заміни дорівнює довжині відкритого тексту. Такі таблиці зручно формувати (і записувати) у вигляді так званих підстановок.

Для зашифрування шифром вертикальної перестановки будується прямокутна таблиця, кількість рядків якої визначається довжиною тексту, а кількість колонок дорівнює довжині ключа. Потім кожна буква ключового слова замінюється на число таким чином, щоб буква, яка має менший порядковий номер в алфавіті, замінювалася на менше число. Отримані числа проставляються підряд на початку відповідних стовпців

таблиці і надалі вважаються номерами цих стовпців. Відкритий текст вписується у таблицю, переходячи звичайним чином з рядка на рядок. Потім виписуються букви зі стовпців таблиці: спочатку весь стовпець, на початку якого стоїть одиниця, потім — стовпець, позначений двійкою і т. д. У підсумку, одержуємо шифротекст.

Створення ключа

Ключем для шифру перестановки буде слугувати гасло — слово «апогей». На основі гасла створюємо таблицю, яка буде використовуватись для шифрування (шкала рознесення). Кількість стовпців у таблиці дорівнює кількості літер у гаслі. Пронумеруємо кожен стовпчик таблиці таким чином, щоб менший порядковий номер літери гасла у алфавіті отримав менше число.

а	п	о	г	е	й
1	6	5	2	3	4

Шифрування

Дано наступний відкритий текст: «Не я належу минулому, а минуле належить мені».

Опускаємо неалфавітні символи тексту і вписуємо його до таблиці послідовно порядково:

а	п	о	г	е	й
1	6	5	2	3	4
н	е	я	н	а	л
е	ж	у	м	и	н
у	л	о	м	у	а
м	и	н	у	л	е
н	а	л	е	ж	и
т	ь	м	е	н	і

Виписуємо літери із стовпців таблиці: у порядку нумерації стовпців, зверху вниз. Отримуємо такий шифротекст (для зручності розбитий на групи по п'ять символів):

неумн тнмму ееаиу лжлнл аеіія уонлм ежлиа ь

Дешифрування

Для розшифрування шифротексту треба виконати обернену послідовність дій: у порядку номерів стовпчиків вписати до таблиці зверху вниз шифротекст і потім вписати послідовно порядково вихідний текст повідомлення.

Висновки

Цей тип шифру є досить давнім і, на відміну від шифрів підстановки, досить стійким. Особливістю є те, що символи відкритого повідомлення не піддаються ніяким перетворенням; натомість вони змінюються своє розташування у тексті відносно інших символів. Визначити використаний алгоритм перестановки є досить складною задачею.

Контрольні запитання

1. *У чому полягає основна суть шифрів перестановки?*

Відмінність цього типу шифру від шифрів заміни полягає в тому, що під час зашифрування буква a_i відкритого тексту переходить не у фіксований знак алфавіту, а в іншу букву того ж відкритого тексту, скажемо a_j , у результаті чого букви розташовуються на нових місцях, тобто переставляються.

2. *Які відмінності між шифрами вертикальної, горизонтальної і подвійної перестановок? Порівняйте їх за складністю і криптографічною якістю.*

Шифри вертикальної та горизонтальної перестановки за складністю використання однакові. За якістю шифрування майже однакові, але в залежності від обраного маршруту записування-зчитування.

Шифр подвійної перестановки більш складний для ручного використання, але забезпечує кращу криптографічну якість, оскільки переміщення відбувається вже у двовимірному просторі, тобто зменшується лінійність.

3. *Які відмітні риси шифрів перестановки? Порівняйте їх із шифрами заміни, кодами.*

На відміну від шифрів заміни та кодів тут використовується той самий набір символів, не відбувається заміна початкового алфавіту.

Немає необхідності зберігати великий ключ співрозмірний із розміром алфавіту, достатньо знати алгоритм, за яким відбувається перестановка.

4. *Поясніть, наскільки криптографічно стійкими є шифри перестановки?*

Зашифрування випадковою, такою, що не має закономірностей, шкалою рознесення при достатньо великій довжині повідомлення робить дешифрування досить проблематичним.

5. *Якими могли б бути способи спрощення побудови ключів шифрів перестановки? Чи знижують ці особливості побудови ключів загальну стійкість застосованого шифру?*

Для спрощення побудови ключів можна скористатись методом гасла, тобто обрати ключову фразу або слово на основі якого буде відбуватись перестановка.

3 Гамування

Теоретичні відомості

Перетворення відкритого тексту часто виконується за допомогою обчислень, здійснюваних над буквами алфавіту, яким попередньо присвоєні деякі числові значення. Наприклад, букви алфавіту нумеруються з нуля, а їхні числові значення збігаються з цими номерами. Для латинського алфавіту букві А можна приписати значення 0, букві В — значення 1, букві С — значення 2 і так далі до букви Z, якій приписується значення, рівне 25. Для того, щоб скласти букви В і D складемо їхні числові значення: $1 + 3 = 4$. Розглянемо суму як числове значення деякої букви латинського алфавіту. Легко бачити, що такою буквою є буква Е. Вважаємо тому: $B + D = E$. При додаванні букви Z з буквою С числове значення дорівнює 27 і, мабуть, не відповідає ніякій букві алфавіту. В таких випадках вважають, що в алфавіті за буквою Z йде буква А, потім В і т. д. У другому алфавіті букві А приписане числове значення рівне 26, букві В — 27 і так до букви Z. Потім йде третій алфавіт, четвертий алфавіт і так далі необхідну кількість разів. Таким чином, можна додавати кілька букв в одному виразі, виконувати множення букв або множити букви на константи. В даному випадку: $Z + C = B$. Зазначені дії над числовими значеннями букв відповідають операціям, виконуваним над числами за модулем m , де модуль дорівнює кількості знаків в алфавіті.

Часто величину m називають модулем алфавіту. Під час виконання модульних операцій однаковим буквам, які знаходяться в різних, послідовно записаних, алфавітах повинні відповідати однакові числові значення. Наприклад, значення 1, 27, 53 задають ту саму букву В і вони, у цьому розумінні, еквівалентні. Неважко бачити, що ці числа відрізняються на величину, кратну m , тобто мають один і той же залишок під час ділення на модуль алфавіту. Такі числа називаються порівнянними за модулем m , що записується у вигляді так званих порівнянь: $a \equiv b \pmod{m}$, тобто $1 \equiv 27 \pmod{26}$, або $1 \equiv 27(26)$. При переході до порівнянь, числові значення і модуль алфавіту маються на увазі, а самі порівняння часто записуються як рівності: $Z + C \equiv B$, замість $Z + C \equiv B \pmod{26}$.

Для отримання шифрованого тексту S існує три способи накладання гами Γ на відкритий текст O : додавання гами і тексту $S = \Gamma + O$, віднімання гами з тексту $S = O - \Gamma$ і віднімання тексту з гами $S = \Gamma - O$. Під операціями додавання і віднімання розуміються як звичайні операції за модулем m , так і застосування замість них відповідних таблиць. Процедура розшифрування, очевидно, будується природним чином, використовуючи обернені перетворення $O = S - \Gamma$, $O = S + \Gamma$, $O = \Gamma - S$ або обернені таблиці, відповідно.

Створення ключа

Для шифрування методом гамування необхідно визначити алфавіт, на основі якого будуть створюватись повідомлення та ключ. Також кожному символу треба надати послідовний номер (код), який буде використовуватись при гамуванні.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

У якості основи гами (ключ) зручно обрати слово-гасло. Нехай це буде «amusement». Сама гама має довжину відкритого повідомлення і складається із повторення гасла.

Шифрування

Необхідно зашифрувати наступний відкритий текст: «Unix is user-friendly. It's just very selective about who its friends are». Приводимо даний текст до канонічного вигляду, тобто відкидаємо усі символи, що відсутні в означеному алфавіті. Отримуємо:

unixisuserfriendlyitsjustveryselectiveaboutwhoitsfriendsare

Складаємо таблицю із трьох рядків. Перший ряд O містить відкрите повідомлення, другий Γ — гаму, третій S — шифрований текст.

За умовою завдання гамування необхідно здійснити за формулою $S = \Gamma - O \pmod{26}$. Це означає, що для отримання поточного символу шифротексту треба від коду відповідного символу гами відняти код відповідного символу відкритого тексту. Таким чином перший символ гами «а», що має код 0, відняти по модулю 26 перший символ відкритого тексту «u» із кодом 20 дає у результаті код 6, тобто символ «g» шифротексту.

В результаті виконання усього процесу гамування отримуємо таблицю:

O	u	n	i	x	i	s	u	s	e	r	f	r	i	e	n	d	l	y	i	t	s	j	u	s	t	v	e	r	y	s
Γ	a	m	u	s	e	m	e	n	t	a	m	u	s	e	m	e	n	t	a	m	u	s	e	m	e	n	t	a	m	u
S	g	z	m	v	w	u	k	v	p	j	h	d	k	a	z	b	c	v	s	t	c	j	k	u	l	s	p	j	o	c
O	e	l	e	c	t	i	v	e	a	b	o	u	t	w	h	o	i	t	s	f	r	i	e	n	d	s	a	r	e	
Γ	s	e	m	e	n	t	a	m	u	s	e	m	e	n	t	a	m	u	s	e	m	e	n	t	a	m	u	s	e	
S	o	t	i	c	u	l	f	i	u	r	q	s	l	r	m	m	e	b	a	z	v	w	j	g	x	u	u	b	a	

Зашифроване повідомлення має такий вигляд:

gzmvwukvpjhdkazbcvstcjkulspjocoticulfiurqslrmmebazvwjgxuuba

Дешифрування

Дешифрування відбувається у зворотньому порядку за формулою $O = \Gamma - S \pmod{26}$. Так перший символ гами «а» (0) відняти по модулю 26 перший символ шифротексту «g» (6) буде 20, тобто «u».

S	g	z	m	v	w	u	k	v	p	j	h	d	k	a	z	b	c	v	s	t	c	j	k	u	l	s	p	j	o	c
Γ	a	m	u	s	e	m	e	n	t	a	m	u	s	e	m	e	n	t	a	m	u	s	e	m	e	n	t	a	m	u
O	u	n	i	x	i	s	u	s	e	r	f	r	i	e	n	d	l	y	i	t	s	j	u	s	t	v	e	r	y	s
S	o	t	i	c	u	l	f	i	u	r	q	s	l	r	m	m	e	b	a	z	v	w	j	g	x	u	u	b	a	
Γ	s	e	m	e	n	t	a	m	u	s	e	m	e	n	t	a	m	u	s	e	m	e	n	t	a	m	u	s	e	
O	e	l	e	c	t	i	v	e	a	b	o	u	t	w	h	o	i	t	s	f	r	i	e	n	d	s	a	r	e	

Після розшифрування отримуємо:

unixisuserfriendlyitsjustveryselectiveaboutwhoitsfriendsare

Розшифроване повідомлення еквівалентне вихідному відкритому повідомленню. Це свідчить про правильність виконання процесів шифрування та дешифрування.

Висновки

Метод гамування не вимагає складної апаратури і громіздких обчислень для забезпечення якісного кодування інформації. Останнім часом метод гамування одержав широке поширення в системах передачі кодованої інформації радіосигналами і телефонного зв'язку. З огляду на високу гнучкість і здатність до модернізації, простоту побудови системи цей метод вибирається за основу багатьох систем захисту.

Контрольні запитання

1. *У чому полягає основна суть шифрування гамуванням?*

Принцип шифрування гамуванням полягає в генерації гами шифру за допомогою генератора псевдовипадкових чисел і накладання одержаної гами на відкриті дані, наприклад, використовуючи додавання за модулем 2.

Процес дешифрування даних зводиться до повторної генерації гами шифру при відомому ключі і накладанні такої гами на зашифровані дані.

2. *Наведіть класифікацію видів гамувальних послідовностей за різними ознаками. Які, у криптографічному розумінні, розбіжності між ними?*

Розрізняють два види гамування — модульне і табличне. Під час табличного гамування вертикальні пари, складені з відповідних знаків відкритого тексту і гами, замінюються на знаки шифртексту за деякою таблицею. Для реалізації взаємооднозначного перетворення така таблиця повинна обов'язково бути так званим «латинським квадратом», тобто будь-який її рядок і будь-який стовпець повинні являти собою перестановку знаків заданого алфавіту, і в кожному стовпці і рядку даної таблиці всі елементи повинні бути різними.

Суть модульного методу полягає в діях над числовими значеннями букв відповідають операціям, виконуваними над числами за модулем m , де модуль дорівнює кількості знаків в алфавіті. Під час виконання модульних операцій однаковою буквам, які знаходяться в різних, послідовно записаних, алфавітах повинні відповідати однакові числові значення. Наприклад, значення 1, 27, 53 задають ту саму букву В і вони, у цьому розумінні, еквівалентні.

3. *Які відмітні риси шифрування гамуванням? Порівняйте його з шифрами заміни, кодами, шифрами перестановки.*

Гамування Накладання на вихідний текст деякої псевдовипадкової послідовності, яка генерується на основі ключа.

Моно- та багато-алфавітні підстановки Заміна символів вихідного тексту на інші (тієї ж абетки) за визначеним правилом. Для забезпечення високої криптостійкості потрібне використання великих ключів.

Перестановки Букви повідомлення не замінюються, а лише переставляються за визначеним алгоритмом. Даний метод використовується звичайно в сполученні з іншими методами.

4. *Поясніть, наскільки криптографічно стійким є шифрування гамуванням і від чого залежить його стійкість?*

Складність і стійкість прямопропорційні в шифруванні гамуванням. Приведемо список видів шифрування гамуванням від найпростішого (найлегшого для зламу) до найскладнішого (найважчого для зламу).

- шифр звичайного накладання двійкової гами,
- шифр багаторазового накладання двійкових гам,
- комбінований шифр Френдберга,
- шифрування тасовкою.

5. *Якими могли б бути способи спрощення побудови послідовності гами? Порівняйте їх зі складністю і криптографічною якістю. Чи знижують їхні особливості загальну стійкість застосованого способу шифрування?*

Для ручного шифрування важливим є легкість запам'ятовування ключа і простота самого процесу дешифрування. Наприклад використання гасел може значно полегшити запам'ятовування ключа.

Чим важче (для розуміння) зашифрувати повідомлення, тим важче його зламати. При спрощенні побудови послідовностей гами спрощується складність і криптографічна якість.

4 Стандарт шифрування даних DES

Теоретичні відомості

DES (англ. Data Encryption Standard) — це симетричний алгоритм шифрування даних, стандарт шифрування прийнятий урядом США із 1976 до кінця 1990-х, з часом набув міжнародного застосування.

Входом у блоковий шифр і результатом його роботи є блок довжиною 64 біти. При необхідності зашифрування повідомлення більшої довжини воно розбивається на блоки, кожен з яких шифрується окремо. Для шифрування використовується ключ довжиною 64 біти.

Процес шифрування представляє собою три етапи: ініціалізацію, 16 однотипних перетворень і завершення. Усі перетворення відбуваються за загально відомими функціями і таблицями.

На етапі ініціалізації вхідний блок даних M піддається IP перетворенню і розбивається на два підблоки L_0 та R_0 . Ключ K шляхом PC-1 перетворення розбивається на два підключі C_0 та D_0 .

У основному циклі виконується послідовне перетворення підблоків та підключів. Вхідними даними наступної ітерації є вихідні дані попередньої. Спочатку формується ключ K_i : C_{i-1} і D_{i-1} зсуваються циклічно вліво на один або два біти (це таблична величина, яка залежить від номера ітерації), і одержаний вектор $C_{i-1}D_{i-1}$ піддається PC-2 перетворенню.

Потім підблок R_{i-1} та ключ K_i передаються до функції Фейстеля. Там підблок розширюється за допомогою E перетворення і складається по модулю 2 із ключем. Сума замінюється деякою послідовністю, яка формується на основі S-блоків. Отримана послідовність є результатом функції.

Результатом ітерації є два нових підблоки $L_i = R_{i-1}$ і $R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$, де f — описана функція Фейстеля.

На завершальному етапі виконується FP (або IP⁻¹) перетворення вектору $R_{16}L_{16}$, а отриманий результат і є зашифрованим блоком.

Створення ключа

Алгоритм шифрування DES використовує ключ довжиною 64 біти, з яких фактично використовується 56 — 7 старших бітів з кожних 8. У якості ключа K візьмемо випадкову послідовність із 64 біт та запишемо її у шістнадцятковому вигляді:

$$K = 11 \text{ eb } \text{ec } 93 \text{ 9c } \text{cb } 9\text{e } 11$$

Шифрування

DES є блоковим алгоритмом. Розмір блока становить 64 біти. Для зручності візьмемо у якості відкритого повідомлення M ASCII-рядок довжиною 8 байт, що як раз складе блок довжиною у 64 біти: «drunkard». У шістнадцятковій формі він має наступний вигляд:

$$M = 64\ 72\ 75\ 6e\ 6b\ 61\ 72\ 64$$

Ініціалізація

Із ключа K за допомогою PC-1 перетворення отримуємо два 28-бітні початкових підключа C_0 і D_0 :

$$C_0 = 01111111\ 0001001\ 1000000\ 1101101$$

$$D_0 = 0110101\ 0010101\ 0001110\ 1101001$$

Із вхідного блоку M за допомогою IP перетворення отримуємо два 32-бітні початкових підблоки L_0 і R_0 :

$$L_0 = 11111111\ 01000110\ 10001101\ 00110100$$

$$R_0 = 00000000\ 11111111\ 00011000\ 01011010$$

Основний цикл

Тепер необхідно послідовно виконати 16 однотипних ітерацій над отриманими початковими підключами та підблоками.

Ітерація № 1 Виконуємо циклічний зсув підключів C_0 та D_0 вліво на 1:

$$C_1 = 11111110\ 0010011\ 0000001\ 1011010$$

$$D_1 = 1101010\ 0101010\ 0011101\ 1010010$$

На основі отриманих нових підключів за допомогою PC-2 перетворення знаходимо 48-бітний ключ K_1 :

$$K_1 = 10011110\ 01110001\ 00001011\ 11011110\ 01000110\ 10101011$$

Виконуємо розширення E підблоку R_0 до 48 біт:

$$R_0^e = 00000000\ 00010111\ 11111110\ 10001111\ 00000010\ 11110100$$

Складаємо по модулю 2 розширений підблок R_0^e і ключ K_1 :

$$R_0^e \oplus K_1 = 10011110 \ 01100110 \ 11110101 \ 01010001 \ 01000100 \ 01011111$$

Виконуємо перетворення отриманого вектору за допомогою S-блоків:

$$S_1 = 00101011 \ 10110101 \ 00110011 \ 11100010$$

Над отриманим результатом виконуємо P перетворення:

$$P_1 = 11100100 \ 00111010 \ 01110111 \ 10000101$$

Знаходимо два результуючих підблоки:

$$L_1 = R_0 = 00000000 \ 11111111 \ 00011000 \ 01011010$$

$$R_1 = L_0 \oplus P_1 = 00011011 \ 01111100 \ 11111010 \ 10110001$$

Ітерація № 2 Виконуємо циклічний зсув підключів C_1 та D_1 вліво на 1:

$$C_2 = 1111100 \ 0100110 \ 0000011 \ 0110101$$

$$D_2 = 1010100 \ 1010100 \ 0111011 \ 0100101$$

На основі отриманих нових підключів за допомогою PC-2 перетворення знаходимо 48-бітний ключ K_2 :

$$K_2 = 00011111 \ 00101011 \ 10000111 \ 00100001 \ 11111101 \ 00100110$$

Виконуємо розширення E підблоку R_1 до 48 біт:

$$R_1^e = 10001111 \ 01101011 \ 11111001 \ 01111111 \ 01010101 \ 10100010$$

Складаємо по модулю 2 розширений підблок R_1^e і ключ K_2 :

$$R_1^e \oplus K_2 = 10010000 \ 01000000 \ 01111110 \ 01011110 \ 10101000 \ 10000100$$

Виконуємо перетворення отриманого вектору за допомогою S-блоків:

$$S_2 = 11101000 \ 11010100 \ 10101000 \ 01001000$$

Над отриманим результатом виконуємо P перетворення:

$$P_2 = 00011101 \ 10011001 \ 10010011 \ 10000000$$

Знаходимо два результуючих підблоки:

$$L_2 = R_1 = 00011011 \ 01111100 \ 11111010 \ 10110001$$

$$R_2 = L_1 \oplus P_2 = 00011101 \ 01100110 \ 10001011 \ 11011010$$

Ітерація № 3 Виконуємо циклічний зсув підключів C_2 та D_2 вліво на 2:

$$C_3 = 1110001 \ 0011000 \ 0001101 \ 1010111$$

$$D_3 = 1010010 \ 1010001 \ 1101101 \ 0010110$$

На основі отриманих нових підключів за допомогою РС-2 перетворення знаходимо 48-бітний ключ K_3 :

$$K_3 = 00111011 \ 00110100 \ 10011001 \ 01101100 \ 00001100 \ 10110110$$

Виконуємо розширення E підблоку R_2 до 48 біт:

$$R_2^e = 00001111 \ 10101011 \ 00001101 \ 01000101 \ 01111110 \ 11110100$$

Складаємо по модулю 2 розширений підблок R_2^e і ключ K_3 :

$$R_2^e \oplus K_3 = 00110100 \ 10011111 \ 10010100 \ 00101001 \ 01110010 \ 01000010$$

Виконуємо перетворення отриманого вектору за допомогою S-блоків:

$$S_3 = 11011111 \ 01111000 \ 10101110 \ 01000010$$

Над отриманим результатом виконуємо P перетворення:

$$P_3 = 01010101 \ 10111011 \ 11000000 \ 11011110$$

Знаходимо два результуючих підблоки:

$$L_3 = R_2 = 00011101 \ 01100110 \ 10001011 \ 11011010$$

$$R_3 = L_2 \oplus P_3 = 01001110 \ 11000111 \ 00111010 \ 01101111$$

Ітерація № 4 Виконуємо циклічний зсув підключів C_3 та D_3 вліво на 2:

$$C_4 = 1000100 \ 1100000 \ 0110110 \ 1011111$$

$$D_4 = 1001010 \ 1000111 \ 0110100 \ 1011010$$

На основі отриманих нових підключів за допомогою РС-2 перетворення знаходимо 48-бітний ключ K_4 :

$$K_4 = 01011101 \ 00000100 \ 11101100 \ 11001101 \ 01001000 \ 11011111$$

Виконуємо розширення E підблоку R_3 до 48 біт:

$$R_3^e = 10100101 \ 11010110 \ 00001110 \ 10011111 \ 01000011 \ 01011110$$

Складаємо по модулю 2 розширений підблок R_3^e і ключ K_4 :

$$R_3^e \oplus K_4 = 11111000 \ 11010010 \ 11100010 \ 01010010 \ 00001011 \ 10000001$$

Виконуємо перетворення отриманого вектору за допомогою S-блоків:

$$S_4 = 00001000 \ 01000110 \ 00111001 \ 11100001$$

Над отриманим результатом виконуємо P перетворення:

$$P_4 = 00110000 \ 01011001 \ 00111100 \ 10000001$$

Знаходимо два результуючих підблоки:

$$L_4 = R_3 = 01001110 \ 11000111 \ 00111010 \ 01101111$$

$$R_4 = L_3 \oplus P_4 = 00101101 \ 00111111 \ 10110111 \ 01011011$$

Ітерація № 5 Виконуємо циклічний зсув підключів C_4 та D_4 вліво на 2:

$$C_5 = 0010011 \ 0000001 \ 1011010 \ 1111110$$

$$D_5 = 0101010 \ 0011101 \ 1010010 \ 1101010$$

На основі отриманих нових підключів за допомогою РС-2 перетворення знаходимо 48-бітний ключ K_5 :

$$K_5 = 11010010 \ 11001000 \ 10011100 \ 00000111 \ 11010010 \ 11011001$$

Виконуємо розширення E підблоку R_4 до 48 біт:

$$R_4^e = 10010101 \ 10101001 \ 11111111 \ 11011010 \ 11101010 \ 11110110$$

Складаємо по модулю 2 розширений підблок R_4^e і ключ K_5 :

$$R_4^e \oplus K_5 = 01000111 \ 01100001 \ 01100011 \ 11011101 \ 00111000 \ 00101111$$

Виконуємо перетворення отриманого вектору за допомогою S-блоків:

$$S_5 = 10100110 \ 00001111 \ 10010001 \ 00011101$$

Над отриманим результатом виконуємо P перетворення:

$$P_5 = 11101011 \ 11000000 \ 00111010 \ 01110000$$

Знаходимо два результуючих підблоки:

$$L_5 = R_4 = 00101101 \ 00111111 \ 10110111 \ 01011011$$

$$R_5 = L_4 \oplus P_5 = 10100101 \ 00000111 \ 00000000 \ 00011111$$

Ітерація № 6 Виконуємо циклічний зсув підключів C_5 та D_5 вліво на 2:

$$C_6 = 1001100 \ 0000110 \ 1101011 \ 1111000$$

$$D_6 = 0101000 \ 1110110 \ 1001011 \ 0101001$$

На основі отриманих нових підключів за допомогою РС-2 перетворення знаходимо 48-бітний ключ K_6 :

$$K_6 = 00011100 \ 10101011 \ 00100110 \ 10010011 \ 10010101 \ 01100101$$

Виконуємо розширення E підблоку R_5 до 48 біт:

$$R_5^e = 11010000 \ 10101000 \ 00001110 \ 10000000 \ 00000000 \ 11111111$$

Складаємо по модулю 2 розширений підблок R_5^e і ключ K_6 :

$$R_5^e \oplus K_6 = 11001100 \ 00000011 \ 00101000 \ 00010011 \ 10010101 \ 10011010$$

Виконуємо перетворення отриманого вектору за допомогою S-блоків:

$$S_6 = 10111111 \ 11111100 \ 01000110 \ 01110000$$

Над отриманим результатом виконуємо P перетворення:

$$P_6 = 01000110 \ 10111101 \ 01010111 \ 01011110$$

Знаходимо два результуючих підблоки:

$$L_6 = R_5 = 10100101 \ 00000111 \ 00000000 \ 00011111$$

$$R_6 = L_5 \oplus P_6 = 01101011 \ 10000010 \ 11100000 \ 00000101$$

Ітерація № 7 Виконуємо циклічний зсув підключів C_6 та D_6 вліво на 2:

$$C_7 = 0110000 0011011 0101111 1100010$$

$$D_7 = 0100011 1011010 0101101 0100101$$

На основі отриманих нових підключів за допомогою РС-2 перетворення знаходимо 48-бітний ключ K_7 :

$$K_7 = 10100010 00111100 00101111 10001010 10001111 10100100$$

Виконуємо розширення E підблоку R_6 до 48 біт:

$$R_6^e = 10110101 01111100 00000101 01110000 00000000 00001010$$

Складаємо по модулю 2 розширений підблок R_6^e і ключ K_7 :

$$R_6^e \oplus K_7 = 00010111 01000000 00101010 11111010 10001111 10101110$$

Виконуємо перетворення отриманого вектору за допомогою S-блоків:

$$S_7 = 01111100 10101011 11100010 00100010$$

Над отриманим результатом виконуємо P перетворення:

$$P_7 = 10000001 01101110 10000111 11010110$$

Знаходимо два результуючих підблоки:

$$L_7 = R_6 = 01101011 10000010 11100000 00000101$$

$$R_7 = L_6 \oplus P_7 = 00100100 01101001 10000111 11001001$$

Ітерація № 8 Виконуємо циклічний зсув підключів C_7 та D_7 вліво на 2:

$$C_8 = 1000000 \ 1101101 \ 0111111 \ 0001001$$

$$D_8 = 0001110 \ 1101001 \ 0110101 \ 0010101$$

На основі отриманих нових підключів за допомогою РС-2 перетворення знаходимо 48-бітний ключ K_8 :

$$K_8 = 11101001 \ 00100110 \ 01100100 \ 01011000 \ 01101111 \ 10010101$$

Виконуємо розширення E підблоку R_7 до 48 біт:

$$R_7^e = 10010000 \ 10000011 \ 01010011 \ 11000000 \ 11111110 \ 01010010$$

Складаємо по модулю 2 розширений підблок R_7^e і ключ K_8 :

$$R_7^e \oplus K_8 = 01111001 \ 10100101 \ 00110111 \ 10011000 \ 10010001 \ 11000111$$

Виконуємо перетворення отриманого вектору за допомогою S-блоків:

$$S_8 = 01110000 \ 11001011 \ 10110111 \ 01111000$$

Над отриманим результатом виконуємо P перетворення:

$$P_8 = 10101011 \ 01110001 \ 10100111 \ 11001010$$

Знаходимо два результуючих підблоки:

$$L_8 = R_7 = 00100100 \ 01101001 \ 10000111 \ 11001001$$

$$R_8 = L_7 \oplus P_8 = 11000000 \ 11110011 \ 01000111 \ 11001111$$

Ітерація № 9 Виконуємо циклічний зсув підключів C_8 та D_8 вліво на 1:

$$C_9 = 0000001 \ 1011010 \ 1111110 \ 0010011$$

$$D_9 = 0011101 \ 1010010 \ 1101010 \ 0101010$$

На основі отриманих нових підключів за допомогою РС-2 перетворення знаходимо 48-бітний ключ K_9 :

$$K_9 = 01110001 \ 10010100 \ 01111110 \ 10100100 \ 10111000 \ 01100101$$

Виконуємо розширення E підблоку R_8 до 48 біт:

$$R_8^e = 11100000 \ 00010111 \ 10100110 \ 10100000 \ 11111110 \ 01011111$$

Складаємо по модулю 2 розширений підблок R_8^e і ключ K_9 :

$$R_8^e \oplus K_9 = 10010001 \ 10000011 \ 11011000 \ 00000100 \ 01000110 \ 00111010$$

Виконуємо перетворення отриманого вектору за допомогою S-блоків:

$$S_9 = 11101100 \ 10101011 \ 11101010 \ 01010011$$

Над отриманим результатом виконуємо P перетворення:

$$P_9 = 10010011 \ 11111110 \ 10001011 \ 11010100$$

Знаходимо два результуючих підблоки:

$$L_9 = R_8 = 11000000 \ 11110011 \ 01000111 \ 11001111$$

$$R_9 = L_8 \oplus P_9 = 10110111 \ 10010111 \ 00001100 \ 00011101$$

Ітерація № 10 Виконуємо циклічний зсув підключів C_9 та D_9 вліво на 2:

$$C_{10} = 0000110 \ 1101011 \ 1111000 \ 1001100$$

$$D_{10} = 1110110 \ 1001011 \ 0101001 \ 0101000$$

На основі отриманих нових підключів за допомогою РС-2 перетворення знаходимо 48-бітний ключ K_{10} :

$$K_{10} = 11100100 \ 11000000 \ 11100010 \ 10100010 \ 10101110 \ 11110110$$

Виконуємо розширення E підблоку R_9 до 48 біт:

$$R_9^e = 11011010 \ 11111100 \ 10101110 \ 10000101 \ 10000000 \ 11111011$$

Складаємо по модулю 2 розширений підблок R_9^e і ключ K_{10} :

$$R_9^e \oplus K_{10} = 00111110 \ 00111100 \ 01001100 \ 00100111 \ 00101110 \ 00001101$$

Виконуємо перетворення отриманого вектору за допомогою S-блоків:

$$S_{10} = 00011000 \ 01001001 \ 01000000 \ 00000111$$

Над отриманим результатом виконуємо P перетворення:

$$P_{10} = 10000000 \ 00001111 \ 00001000 \ 01100010$$

Знаходимо два результуючих підблоки:

$$L_{10} = R_9 = 10110111 \ 10010111 \ 00001100 \ 00011101$$

$$R_{10} = L_9 \oplus P_{10} = 01000000 \ 11111100 \ 01001111 \ 10101101$$

Ітерація № 11 Виконуємо циклічний зсув підключів C_{10} та D_{10} вліво на 2:

$$C_{11} = 0011011 \ 0101111 \ 1100010 \ 0110000$$

$$D_{11} = 1011010 \ 0101101 \ 0100101 \ 0100011$$

На основі отриманих нових підключів за допомогою РС-2 перетворення знаходимо 48-бітний ключ K_{11} :

$$K_{11} = 10110010 \ 11001011 \ 00110110 \ 00111101 \ 10001111 \ 10010011$$

Виконуємо розширення E підблоку R_{10} до 48 біт:

$$R_{10}^e = 10100000 \ 00010111 \ 11111000 \ 00100101 \ 11111101 \ 01011010$$

Складаємо по модулю 2 розширений підблок R_{10}^e і ключ K_{11} :

$$R_{10}^e \oplus K_{11} = \\ 00010010 \ 11011100 \ 11001110 \ 00011000 \ 01110010 \ 11001001$$

Виконуємо перетворення отриманого вектору за допомогою S-блоків:

$$S_{11} = 11010100 \ 11111010 \ 00010010 \ 10011010$$

Над отриманим результатом виконуємо P перетворення:

$$P_{11} = 00101110 \ 11100011 \ 10000001 \ 01010111$$

Знаходимо два результуючих підблоки:

$$L_{11} = R_{10} = 01000000 \ 11111100 \ 01001111 \ 10101101$$

$$R_{11} = L_{10} \oplus P_{11} = 10011001 \ 01110100 \ 10001101 \ 01001010$$

Ітерація № 12 Виконуємо циклічний зсув підключів C_{11} та D_{11} вліво на 2:

$$C_{12} = 1101101 \ 0111111 \ 0001001 \ 1000000$$

$$D_{12} = 1101001 \ 0110101 \ 0010101 \ 0001110$$

На основі отриманих нових підключів за допомогою РС-2 перетворення знаходимо 48-бітний ключ K_{12} :

$$K_{12} = 10101100 \ 00110011 \ 00010011 \ 00011111 \ 01000100 \ 01010011$$

Виконуємо розширення E підблоку R_{11} до 48 біт:

$$R_{11}^e = 01001111 \ 00101011 \ 10101001 \ 01000101 \ 10101010 \ 01010101$$

Складаємо по модулю 2 розширений підблок R_{11}^e і ключ K_{12} :

$$R_{11}^e \oplus K_{12} = \\ 11100011 \ 00011000 \ 10111010 \ 01011010 \ 11101110 \ 00000110$$

Виконуємо перетворення отриманого вектору за допомогою S-блоків:

$$S_{12} = 00111011 \ 01100010 \ 11110011 \ 00000100$$

Над отриманим результатом виконуємо P перетворення:

$$P_{12} = 01100001 \ 01101101 \ 01100010 \ 10100110$$

Знаходимо два результуючих підблоки:

$$L_{12} = R_{11} = 10011001 \ 01110100 \ 10001101 \ 01001010$$

$$R_{12} = L_{11} \oplus P_{12} = 00100001 \ 10010001 \ 00101101 \ 00001011$$

Ітерація № 13 Виконуємо циклічний зсув підключів C_{12} та D_{12} вліво на 2:

$$C_{13} = 0110101 \ 1111100 \ 0100110 \ 0000011$$

$$D_{13} = 0100101 \ 1010100 \ 1010100 \ 0111011$$

На основі отриманих нових підключів за допомогою РС-2 перетворення знаходимо 48-бітний ключ K_{13} :

$$K_{13} = 00100111 \ 00010110 \ 01111101 \ 01001111 \ 11100001 \ 01000100$$

Виконуємо розширення E підблоку R_{12} до 48 біт:

$$R_{12}^e = 10010000 \ 00111100 \ 10100010 \ 10010101 \ 10101000 \ 01010110$$

Складаємо по модулю 2 розширений підблок R_{12}^e і ключ K_{13} :

$$R_{12}^e \oplus K_{13} = \\ 10110111 \ 00101010 \ 11011111 \ 11011010 \ 01001001 \ 00010010$$

Виконуємо перетворення отриманого вектору за допомогою S-блоків:

$$S_{13} = 00011000 \ 10011001 \ 01011111 \ 10111001$$

Над отриманим результатом виконуємо P перетворення:

$$P_{13} = 10111110 \ 00101100 \ 00101101 \ 01001011$$

Знаходимо два результуючих підблоки:

$$L_{13} = R_{12} = 00100001 \ 10010001 \ 00101101 \ 00001011$$

$$R_{13} = L_{12} \oplus P_{13} = 00100111 \ 01011000 \ 10100000 \ 00000001$$

Ітерація № 14 Виконуємо циклічний зсув підключів C_{13} та D_{13} вліво на 2:

$$C_{14} = 1010111 \ 1110001 \ 0011000 \ 0001101$$

$$D_{14} = 0010110 \ 1010010 \ 1010001 \ 1101101$$

На основі отриманих нових підключів за допомогою РС-2 перетворення знаходимо 48-бітний ключ K_{14} :

$$K_{14} = 11001111 \ 01010000 \ 11010000 \ 10100000 \ 11100101 \ 11001100$$

Виконуємо розширення Е підблоку R_{13} до 48 біт:

$$R_{13}^e = 10010000 \ 11101010 \ 11110001 \ 01010000 \ 00000000 \ 00000010$$

Складаємо по модулю 2 розширений підблок R_{13}^e і ключ K_{14} :

$$R_{13}^e \oplus K_{14} = \\ 01011111 \ 10111010 \ 00100001 \ 11110000 \ 11100101 \ 11001110$$

Виконуємо перетворення отриманого вектору за допомогою S-блоків:

$$S_{14} = 10110101 \ 10000011 \ 00001000 \ 11000001$$

Над отриманим результатом виконуємо Р перетворення:

$$P_{14} = 10010000 \ 11010000 \ 01001011 \ 00010011$$

Знаходимо два результуючих підблоки:

$$L_{14} = R_{13} = 00100111 \ 01011000 \ 10100000 \ 00000001$$

$$R_{14} = L_{13} \oplus P_{14} = 10110001 \ 01000001 \ 01100110 \ 00011000$$

Ітерація № 15 Виконуємо циклічний зсув підключів C_{14} та D_{14} вліво на 2:

$$C_{15} = 1011111 \ 1000100 \ 1100000 \ 0110110$$

$$D_{15} = 1011010 \ 1001010 \ 1000111 \ 0110100$$

На основі отриманих нових підключів за допомогою РС-2 перетворення знаходимо 48-бітний ключ K_{15} :

$$K_{15} = 00011110 \ 11001011 \ 11111000 \ 11101000 \ 10010110 \ 10000111$$

Виконуємо розширення E підблоку R_{14} до 48 біт:

$$R_{14}^e = 01011010 \ 00101010 \ 00000010 \ 10110000 \ 11000000 \ 11110001$$

Складаємо по модулю 2 розширений підблок R_{14}^e і ключ K_{15} :

$$R_{14}^e \oplus K_{15} = \\ 01000100 \ 11100001 \ 11111010 \ 01011000 \ 01010110 \ 01110110$$

Виконуємо перетворення отриманого вектору за допомогою S-блоків:

$$S_{15} = 10100100 \ 10010010 \ 11110100 \ 00101101$$

Над отриманим результатом виконуємо P перетворення:

$$P_{15} = 00101101 \ 11000100 \ 00001111 \ 10111000$$

Знаходимо два результуючих підблоки:

$$L_{15} = R_{14} = 10110001 \ 01000001 \ 01100110 \ 00011000$$

$$R_{15} = L_{14} \oplus P_{15} = 00001010 \ 10011100 \ 10101111 \ 10111001$$

Ітерація № 16 Виконуємо циклічний зсув підключів C_{15} та D_{15} вліво на 1:

$$C_{16} = 0111111 0001001 1000000 1101101$$

$$D_{16} = 0110101 0010101 0001110 1101001$$

На основі отриманих нових підключів за допомогою РС-2 перетворення знаходимо 48-бітний ключ K_{16} :

$$K_{16} = 10100111 11001001 10010001 00101011 10110001 01111000$$

Виконуємо розширення E підблоку R_{15} до 48 біт:

$$R_{15}^e = 10000101 01010100 11111001 01010101 11111101 11110010$$

Складаємо по модулю 2 розширений підблок R_{15}^e і ключ K_{16} :

$$R_{15}^e \oplus K_{16} = \\ 00100010 10011101 01101000 01111110 01001100 10001010$$

Виконуємо перетворення отриманого вектору за допомогою S-блоків:

$$S_{16} = 00100011 11101100 01101111 11111111$$

Над отриманим результатом виконуємо P перетворення:

$$P_{16} = 01011010 00110111 01111111 11101101$$

Знаходимо два результуючих підблоки:

$$L_{16} = R_{15} = 00001010 10011100 10101111 10111001$$

$$R_{16} = L_{15} \oplus P_{16} = 11101011 01110110 00011001 11110101$$

Завершення

Виконуємо FP перетворення над вектором $R_{16}L_{16}$ і отримуємо остаточні 64 біти шифру, що у шістнадцятковій формі мають вигляд:

$$M' = 4f \ d8 \ 39 \ ee \ 37 \ 5b \ 51 \ 6b$$

Перевірка

Робимо перевірку зашифрованого блоку шляхом розшифрування за допомогою стороннього незалежного та авторитетного ПО, наприклад, `openssl`:

```
$ echo -en '\x4f\xd8\x39\xee\x37\x5b\x51\x6b' | \
  openssl des-ecb -nosalt -nopad -d -iv 0 \
  -K 11ebec939ccb9e11; echo
drunkard
```

Розшифрований текст еквівалентний початковому. Це свідчить про правильно виконану процедуру зашифрування.

Висновки

Зараз DES вважається ненадійним в основному через малу довжину ключа (56 біт) та розмір блоку (64 біти). У 1999 ключ DES було публічно дешифровано за 22 години 15 хвилин. Вважається, що алгоритм достатньо надійний для застосування у модифікації 3-DES, хоча існують розроблені теоретичні атаки. DES поступово витісняється алгоритмом AES, що з 2002 року є стандартом США.

Контрольні запитання

1. *У чому полягає основна суть і необхідність появи «блокових» шифрів?*

Особливістю блочного шифру є обробка блоку декількох байт за одну ітерацію (як правило 8 або 16). Робота блочного шифру в найпростішому режимі — застосування функції, що шифрує, до блоку даних (проста заміна) викликає серйозну проблему: статистичні властивості відкритих даних частково зберігаються, тому що кожному однаковому блоку даних однозначно відповідає зашифрований блок даних. При великій кількості даних (відео, звук) це може дати деякі відомості для криптоаналізу про зміст даних. Для вирішення вищеописаних проблем, використовується циклічне перетворення, яке повинно використовувати наступні принципи:

Розсіювання Тобто зміна будь-якого знака відкритого тексту або ключа впливає на велику кількість знаків шифротекста, що приховує статистичні властивості відкритого тексту;

Переміщення Використання перетворень, ускладнюють отримання статистичних залежностей між шифротекстом і відкритим текстом.

2. *Що є основним елементом шифру DES?*

Основними елементами є блок даних розміром 64 біти і ключ розміром 56 біт.

3. *Поясніть суть циклової функції $f(R, K)$.*

Суть функції полягає у створенні закодованого блоку даних за допомогою R перетворення та підстановки S -блоків на основі ключу.

4. *Які головні вимоги до S -блоків ви б сформулювали, якби постала задача про їх заміну?*

Нелінійність перетворень в DES засобами тільки S -блоків, у випадку, якщо вони мають слабіну, дозволяє здійснювати контроль за шифрованим листуванням. Вибір S -блоків вимагає дотримання кількох умов:

- Кожен рядок кожного блоку повинен бути перестановкою множини $0, 1, 2, \dots, 15$.
- S -блоки не повинні бути лінійної або афінною функцією своїх аргументів.
- Зміна одного біта на вході S -блоку повинно приводити до зміни принаймні двох бітів на виході.
- Для кожного S -блоку і будь-якого аргументу x значення $S(x)$ та $S(x \oplus 001100_2)$ повинні відрізнятися принаймні двома бітами.

5. *Наскільки криптографічно стійким є шифрування даним блоковим шифром? Що впливає і може впливати на його стійкість? Як?*

На сьогоднішній день DES вважається нестійким, оскільки, поперше, розмір ключа — 56 бітів — замалий, тому існує реальна загроза пошуку ключа лобовою атакою (послідовним перебором); подруге, DES нестійкий до лінійного криптоаналізу (тобто лінійна атака дозволяє знайти ключ DES швидше, ніж послідовний перебір). Через невелику кількість можливих ключів (всього 2^{56}), з'являється можливість їх повного перебору на швидкодійній обчислювальній техніці за реальний час. У 1998 році The Electronic Foundation використовуючи спеціальний комп'ютер DES-Cracker, вдалося зламати DES за 3 дні.

6. Які режими використання алгоритму шифрування DES?

Для DES рекомендовано кілька режимів:

- режим електронної кодової книги (ECB — Electronic Code Book),
- режим зчеплення блоків (CBC — Cipher Block Chaining),
- режим зворотнього зв'язку по шіфротексту (CFB — Cipher Feed Back),
- режим зворотнього зв'язку по виходу (OFB — Output Feed Back).

Література

1. Хорошко В. О., Азаров О. Д., Шелест М. Є., Андреев В. І., Щербина В. П., Яремчук Ю. Є. Комп'ютерна криптографія. Лабораторний практикум. — К.: НАУ, 2003. — 94 с.
2. J. Orlin Grabbe. The DES Algorithm Illustrated. — <http://orlingrabbe.com/des.htm>
3. <http://en.wikipedia.org>