Горпенюк Андрій Ярославович

Методи та засоби криптологічних перетворень

Зміст

[Тема: Вступ. Криптологія. Історія криптології 2](#_Toc256686539)

[1. Історія криптології 2](#_Toc256686540)

[Шифр Цезаря 2](#_Toc256686541)

[Шифр Скитала 3](#_Toc256686542)

[Інші: диск Енея, книжний шифр, квадрат Полібія, тюремний шифр, шифр загорожі 3](#_Toc256686543)

[2. Основні поняття та визначення криптології 5](#_Toc256686544)

[Відкрите та закрите шифруванн 5](#_Toc256686545)

[Симетричні і асиметричні алгоритми 6](#_Toc256686546)

[Задачі криптографії 7](#_Toc256686547)

[Стійкість алгоритмів 8](#_Toc256686548)

[Складність алгоритму 8](#_Toc256686549)

[Класичні криптосистеми та їх криптоаналіз 9](#_Toc256686550)

[Шифри простої заміни 9](#_Toc256686551)

[Криптоаналіз шифру прострої заміни 10](#_Toc256686552)

[Частотний криптоаналіз 10](#_Toc256686553)

[Гомофонний шифр заміни 11](#_Toc256686554)

[Поліграмні шифри 12](#_Toc256686555)

[Шифр Playfair’а 12](#_Toc256686556)

[Поліалфавітні криптосистеми 12](#_Toc256686557)

Лекція №2

2010-02-24

# Тема: Вступ. Криптологія. Історія криптології

**Криптологія** – це наука, яка охоплює 2 взаємопов’язалані частини: *криптографію* та *криптоаналіз*.

*Криптографія* – це наука про зовнішню зміну інформації без зміни її змісту до такого вигляду, щоб цей зміст став недоступний для непосвячених споживачів. При цьому сам факт існування інформації як правило не приховується. Основна мета: погіршення розуміння інформації, що принципово розрізняє її від кодування.

*Стеганографія* – це наука про приховування інформації

*Криптоаналіз* – це наука про методи розкриття шифру, тобто про розкриття змісту без знання ключа.

## 1. Історія криптології

Здавна відомі 3 захисти:

1. Фізичний
2. Стеганографія (від гр. «тайнопис») – одна з перших згадок в працях давньогрецького історика *Геродота*(«голова раба» - голову брили, писали надпис, волосся відрощували і відправляли адресату).

Особливого розвитку набули в кінці 20го століття разом з розвитком інформаційних технологій. Таємні повідомлення стали розповсюджувати у відкритих файлах, які передавалися через всесвітню мережу, наприклад у відео-, фото-, аудіофайлах

1. Перетворення змістовного тексту в нечитабельний набір символів, при чому отримувач знає метод оберного перетворення.

В документах Індії, Єгипту, Мессопотамії є відомості про способи складання шифрованих повідомлень. Зокрема в давньоіндійських джерелах описано 64 способи таємного письма, один з найдавніших шифрованих текстів походить з Мессопотамії, це є шифрований рецепт виготовлення глазурі до гончарних виробів.

В давньоєгипетських джерелах застосовувались релігійні шифровані тексти, рецепти і надгробні епітафії. Особливо методи розвинулись завдяки власне цим епітафіям. Єгиптяни заставили прохожих прочитати цей надпис велику кількість разів, і так показати свою вдячність мрецю)) Вийнятком в часи давніх цивілізації з т.з. криптології були цивілізації із складним письмом. Зокрема в Китаю нема жодних згадок про криптологію. Оскільки письмо було таким складним, що володіли ним обрані і не потрібно було розробляти будь-які методи шифрування.

### Шифр Цезаря

Найвідоміші та достовірні дані про шифри мають стосунок до Давної Греції, Священної Римської Імперії. Найвідомішим історичним прикладом шифроу є шифр *Юльки Цезарівни*, 1ст до н.е. Він описаний істориком давнього Риму – Святонієм. Цезар при шифруванні кожну букву відкритого тексту заміняв іншую буквою, а саме такою, яка на кілька символів відрізнялася від попередньої. Шифр Цезара – це перший приклад шифру **зсуву** (заміни). До сьогоднішніх днів він є одним із базових методів в криптографії. Кажуть що цей шифр є шифром зсуву на 3 позиції. Цей та інші шифри зручно задавати таблицею, у верхньому рядку якої є алфавіт, у якому пишуть повідомлення, нижнім рядком – цей же алфавіт, але зсунутий на певну кількість позицій. Наприклад, стосовно української абетки, така таблиця мала б наступний вигляд:

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| а | б | в | г | ґ | д | е | є | ж | ... | ь | ю | я |
| г | ґ | д | е | є | ж | з | и | і | ... | а | б | в |

Ключем в шифрі є величина зсуву.

*Жили були дід та баба їли кашу з молоком, розвернувся дід на бабу і ударив кулаком. Баба плакала, ридала діда клятого прокляла. А він плакав теж, бо знав, що це станеться... тьху, рими нема)))*

### Шифр Скитала

Іншим відомим шифром тих часів і одночасно шифруючим пристроєм був т.зв. шифр **«Скитала»**, винайдений в давній Спарті, римляни також перейняли його і широко використовували для військових дій. Брали пергаментну стрічку, намотували на стержень і писали впоперек. Це шифр **перестановки**. До сьогоднішнього дня симетричні шифри – це комбінація цих двох методів кодування. Особливістю шифрів – букви повідомлення в зашифрованому тексті зберігаються, просто переходять на іншні позиції. Цікаво, що винайденя дешифруючого пристроя (антискитала) приписують Арістотелю. Він для розшифрування повідомлення брав спис з наконечником змінного діаметру. Намотував стрічку на цей спис, змінюючи таким чином діаметр, добивався того, щоб вздовж осі читався текст. Ключем шифра Скитала є діаметр Скитала

### Інші: диск Енея, книжний шифр, квадрат Полібія, тюремний шифр, шифр загорожі

Давньогрецький полководець *Еней Тактика* в 4му ст. до н.е. запропонував пристрій, який назвали диском Енея – це диск, з проставленими в ньому отворами. В кожному отворі була проставлена буква. Відповідність знали лише отримувач і відправник. В центрі була нитка, яка витягувалась і протягувалась через отвори. Диск з протягнутою ниткою відсилався. Замість диску ще можна було використати лінійку.

Еней Тактика також запропонував застосовувати книжний шифр, тобто над певними буквами якогось документу проколювати малозамітні отвори, які позначали букви таємного повідомлення, тобто це більше був стеганографічний метод. Такий метод з успіхом застосовувався в часах *1ї Світової війни*.

В сучасному розумінні книжний шифр є інший шифр, в якому ключем є певна сторінка певної книги, а кожна буква відкритого повідомлення шифрується номером рядка і номером букви в рядку на цій сторінці. Таке застосовували в часи *2ї Світової війни*.

Квадрат Полібія – для латинського алфавіту, в якому вилучено букву j, яка найменше застосовується, має такий вигляд:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | A | B | C | D | E |
| A | A | B | C | D | E |
| B | F | G | H | I | K |
| C | L | M | N | O | P |
| D | Q | R | S | T | U |
| E | V | W | X | Y | Z |

Для кращого шифрування в першому рядку/стопці записували ключове слово, після чого квадрат Полібія відновлювався. Сучаним варіантом є т.зв. тюремний шифр, в якому букви передавалися стуком. Ним можна подати номер рядка і номер стовпця.

Є відомості про інший шифр простої заміни і шифруючий пристрій, який застосовували римляни. Цей пристій складався з двох дисків на одній осі. На одному диску були написані букви алфавіту в природньому порядку, на другому в зміненому порядку. При шифруванні записували букви по другому диску. Для дешифровки треба було знати зсув.

Після середньовіччя – це занепад криптографічних методів.

Відродження – почала активно розвиватись культура, писемність, відповідно знову почались розвиватися криптологічні методи. В часи відродження, поряд з традиційним застосуванням криптографії в політиці і військовій справі, криптографічні методи починають широко застосовуватися для захисту інтелектуальної власності – від переслідування інквізицією та кражі конкерентами. Це наближає тодішню криптографію до криптографії сучасної. В ці часи починають застосовувати так званий шифр загорожі.

Повідомлення описують у вигляді загорожі певної висоти, зліва направо, зверху вниз. Наприклад, повідомлення «інформацію отримав» шифром загорожі 3го порядку можна зашифрувати наступним чином.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Ф |  |  |  | А |  |  |  | О |  |  |  | М |  |  |
|  | Н |  | О |  | М |  | Ц |  | Ю |  | Т |  | И |  | А |  |
| І |  |  |  | Р |  |  |  | І |  |  |  | Р |  |  |  | В |

Записують ФАОМНОМЦЮТИАІРІРВ.

Леон Батіст Альберті винайнов метод багатоалфавітної заміни. Саме такий метод і є основою сучасних шифрів. Цей метод вдосконалив і дав йому своє ім’я Блейз Віженер(дипломат 16го ст.). Різні композиції шифру Віженера застосовувалися аж до середини 20го ст. Зокрема відомий німецький шифр Енігма є ніщо іншим, як композицією шифра Віженера.

Той самий Альберті в 1466р. написав першу в світі наукову працю з криптографії *«Трактат про шифр»*.

1508р. – німецький аббат Іоган Трисемус видав першу друковану працю з криптогрфії, яка називалася *«Поліграфія»*.

Саме Альберті вперше запропонував застосовувати квадрат Полібія з ключовим словом для т.зв. шифрування біграмами.

Давінчі застосовував письмо-навпаки.

## 2. Основні поняття та визначення криптології

Класична задача криптології виникає тоді, коли двоє людей, а в загальному випадку – 2 сторони збираються обмінюватися секретною інформацією за пристуності третьої, недружньої сторони, яка намагається заволодіти цією інформацією.

За традицією, що встановилася в криптографічній літературі, перші дві сторони називають *Алісою* та *Бобом*. Третю сторону називають *суперником*.

Аліса, як правило, передає конфіденційну інформацію, а Боб приймає. Суперника називають часто *Євою*– це перехоплювач повідомлень. Або *Мелорі* – зловмисник, активний зламувач шифрів.

З точки зору сучасних інформаційних і телекомунікаційних технологій, Аліса і Боб є легальними, Єва або Мелорі – несанкціонований користувач по каналам зв’язку. Щоб зберегти таємницю, Аліса ***зашифровує*** своє повідомлення – тобто застосувавши якийсь алгоритм *зашифрування*, перетворює його до незрозумілої для суперника форми. В результаті з повідомлення, яке ще називають відкритим текстом, Аліса отримує крипто-текст або шифро-текст. Часто поняття відкритого повідомлення і відкритого тексту розділяють. Відкрите повідомлення позначають буквою **M** (від англ. message) і розуміють під ним будь-яку інформацію(текст, потік бітів, оцифрований звук, графічне оцифроване зображення). Термін «Відкритий текст» вживають, якщо необхідно підкреслити, що це є дійсно текст якоюсь мовою, позначають **P** (від англ. *Plain Text* – звичайний текст).

Озн. Процес заміни форми повідомлення способом, що дозволяє приховати його зміст називають зашифруванням. Зашифроване повідомлення називається шифро-текстом або крипто-текстом.

Озн. Процедура зворотнього перетворення називається розшифруванням

Разом з тим термін шифрування часто вживають до обох процесів – зашифрування, розшифрування, але й розшифрування часто вживається в сенсі розшифрування. Боб отримує криптотекст і розшифровує його за допомогою аглоритму розшифрування. В результаті отримує вихідне відкрите повідомлення.

Озн. Алгоритми розшифрування та зашифрування разом складають алгоритм шифрування або частину шифру.

Науку і мистецтво створення шифрів називають **криптографією**. Криптоаналіз – наука взламу шифру, спеціалісти – криптоаналітики.

Криптоаналітики намагаються здійснити ***дешифрування*** – тобто відновити зміст повідомлення без знання таємних параметрів ключа(таємних параметрів шифру).

Розділ математики, що охоплює криптографіку та криптоаналіз – **криптологія**. Спеціалісти, які займаються цією наукою називають криптологами.

### Відкрите та закрите шифруванн

Якщо рівень захисту інформації, що забезпечується алгоритмом шифрування, залежить від збереження цього алгоритму в таємниці, то алгоритм називають *обмеженим*. До другої половини 20го століття використовували його. Обмеження алгоритмів не витримують зміни абонентів, не допускають ефективного контролю та стандартизації, застосування відкритих програмних чи апаратних продуктів.

Надійнішим і зручнішим є застосування *відкритих* алгоритмів шифрування. Такі алгоритми в деталях відомі всі. При застосуванні відкритих алгоритмів, конфіденційність забезпечується застосуванням таємного параметру шифру, такий параметр називають ключем і позначають буквою **K**.Наприклад в шифрі Цезаря – це величина зсуву, в шифрі Скитала – діаметр скитала. Аліса і Боб домовляються про таємний ключ наперед, тобто обмінюються ключем, або застосовують кожен свій таємний ключ. Цей ключ вони зберігають в таємниці від суперника і часто міняють. Можину всіх можливих ключів називають *простором ключів*. Аналогічно визначають простори відкритих повідомлень та шифротекстів.

Озн. Криптосистема (або **шифр**) – це алгоритм шифрування, (який включає алгоритм зашифрування і розшифрування) плюс всі відкриті тексти, шифротексти та ключі.

Із застосуванням цих понять нарисуємо структурку класичної криптографічної схемки:



E,D – зашифрування, розшифрування

K – ключ, який може бути на обох сторонах різним

C – шифротекст

, який є результатом зашифрування

, дешифрування з ключем шифротекста, маємо на виході повідомлення

Якщо застосовані два ключі, то

Аналізуючи надійність шифрів, побудованих на відкритих алгоритмах, виходять з припущення, що суперник не тільки здатний слухати криптотекст, але в деталях знає алгоритми зашифруванні і розшифрування, в деталях ключ K йому не відомий.

### Симетричні і асиметричні алгоритми

Відомо два основні типи алгоритму, заснованих на застосування ключів: симетричні алгоритми шифрування та асиметричні алгоритми шифрування.

***Симетричні*** називають алгоритми із секретним, таємним ключем, або алгоритми з єдиним (спільним) ключем. Вимагають щоб Аліса і Боб перед початком передавання даних узгодили єдиний таємний для суперника ключ. Якщо в симетричній системі ключі зашифрування/розшифрування – різні, тоді ключ розшифрування можна легко обчислити з ключа зашифрування.

Симетричні алгоритми ділять на 2 категорії:

* потокові алгоритми(шифри) – обробляють відкритий текст побітово;
* блочні алгоритми(блокові шифри) – обробляють групи бітів відкритого тексту. Такі групи називають блоками.

***Асиметричні*** алгоритми шифрування(алгоритми з відкритим, або публічним ключем) передбачають наявність двох різних ключів, - відкритого(публічного) ключа зашифрування та закритого(таємного) ключа розшифрування, при чому ключ розшифрування дуже тяжко обчислити із зашифрування. Отже в таких системах Боб відкрито публікує ключ, будь-хто може дізнатись ключ і зашифрувати своє повідомлення. Але розшифрувати це повідомлення можна лише знаючи таємний ключ.

Часто асиметричні алгоритми застосовують в режимі, коли зашифрування здійснюється таємним ключем відправника, розшифрування: відкритим ключем відправника, такий режим називають режимом цифрового підпису.

## Задачі криптографії

Основна задача криптогрфії – забезпечення конфіденційності. Крім цього криптографічні алгоритми застосовують для вирішення інших задач, зокрема:

* цілісність – отримувач повинен мати можливість перевірити чи не було повідомлення змінене в процесі доставки, а суперник не здатний видати змінене повідомлення за справжнє;
* перевірка оригінальності (аутентифікації) – отримувач повинен мати можливість встановити джерело повідомлень, а суперник не здатний замаскуватися під когось іншого
* незаперечення авторства – відправник не повинен мати можливості заперечувати згодом відправку повідомлень

Основна задача криптоаналітика – відновити зміст повідомлення M. Згідно традиційної криптографічної термінології суперник здійснює атаку на шифр. Успішний криптоаналіз дозволяє відновити відкритий текст або ключ. Крім того криптоаналіз дозволяє виявити слабкі місця в криптосистемі.

Озн. Розкриття ключа без застосування методів криптології називають ***компроментацією*** ключа.

Відомо 4 основні типи криптоаналітичних атак (для відкритих):

1. Атака на основі **лише шифр-тексту**. Тут криптоаналітик має в своєму розпорядженні шифр-текст одного або декількох повідомлень, зашифрованих одним алгоритмом. Його задача – дешифрування якомога більшої кількості повідомлень. Ще краще якщо він встановить ключ зашифрування

Дано:

Знайти: відкритий текст або ключ , або алгоритми відновлення з

1. Атака з **відомим** відкритим текстом – криптоаналітик має доступ не тільки до відомих шифрів тексту, але й до відкритих текстів. Тобто відкриті тексти зашифрованих він також має.

Дано:

Знайти: і читати наступні повідомлення, або з

1. Атака з **вибраним** відкритим текстом – криптоаналітик має ряд шифротекстів відповідних їм відкритих текстів, а також можливість вибирати відкритий текст для зашифрування
2. Атака з **адаптивно-підібраним** відкритим текстом – криптоаналітик може не тільки вибирати відкритий текст для зашифрування, але й уточняти кожен свій наступний вибір, спираючись на попеердні результати розшифрування.

Крім цих видів атак відомо ще щонайменше 3 типи атак

1. Атака з вибраним шифр-текстом – аналітик може вибирати різні шифр-тексти для розшифрування (на якийсь час отримав доступ до обладнання і автоматично здійснює розшифрування). Задача полягає в розкритті ключа.
2. Атака з підібраним ключем – криптоаналітику відомі певні зв’язки між різними ключами
3. Бандитський – вкрасти, вибирти, купити, набити мордяку, закопати до смерті, це все дуже ефективні методи. Особливо, якщо застосовувати їх з логічно-випитувальним методом із застосування деприсивно-психологічних чинників на цю особу.

# Стійкість алгоритмів

Залежно від складності взлому різні криптоалгоритми забезпечують різну стійкість, при чому цю стійкість можуть оцінювати по різному. Якщо вартість взлому більша за вартість даних, тоді це не вигідно. Так само якщо час, який затрачається на взлом більший за термін дії даних, то у взломі немає сенсу.

Відома така класифікація складності взлому, в порядку спадання значущості:

1. **Повне розкриття** (повна ганьба *(C)Мазур*). У цьому випадку криптоаналітик знаходить ключ K, щоб
2. **Глобальна дедукція**. Криптоаналітик знаходить альтернативний криптоалгоритм A, еквівалентний без знання ключа K.
3. **Випадкова(часткова) дедукція**. Криптоаналітик знаходить відкритий текст для перехопленого шифр-тексту, наприклад, краде, випитує, вибиває мозґи з тушки його і мордяку розчавлює в асфальт, як в *Manhunt*.
4. **Інформаційна дедукція**. Криптоаналітик вибуває деяку інформацію про ключ або відкритий текст. Це можуть бути, наприклад, декілька бітів ключа або деяка відомость про внутрішній зміст тексту.

Алгоритм **безумовно стійкий**(або стійкий в інформаційному сенсі), якщо відновлення відкритого тексту неможливе при будь-якому об’ємі перехопленого шифр-тексту. Існує(доведено Шенноном) єдиний абсолютно стійкий шифр. Всі інші шифри можуть бути розкриті з використанням тільки шифр-тексту простим перебором всіх можливих ключів і перевіркою осмисленості отриманого відкритого тексту.

Такий метод називають брутальною(або лобовою, *brute force*) атакою. Алгоритм називається стійким в обчислювальному сенсі, якщо не може бути розкритий за прийнятий час і застосуванням доступних обчислювальних потужностей.

## Складність алгоритму

Складність тої чи іншої атаки оцінюють різними способами:

1. За складністю даних, тобто за об’ємом вихідних даних, необхідних для успішної атаки.
2. За складністю обробки, тобто за часом, необхідним для здійснення атаки. Часто таку оцінку називають *фактором трудозатрат*.
3. За вимогами до пам’яті комп’ютера, тобто за об’ємом пам’яті необхідним для успішної атаки.

Приблизна складність алгоритму визначається максимальною оцінкою, пораховану за кожним із цих трьох факторів.

Складність алгоритмів прийнято порівнювати порядками величин. Наприклад, якщо відомо, що складність алгоритму визначається як складністю в .

Озн. 1. Довільно скінченну непросту множину називають *алфавітом*.

Озн.2. Елементи алфавіту називають *буквами*.

Озн.3. Будь-які кінцеві послідовності елементів алфавіту (букв) називають *словами*.

Озн.4. Слово, що містить 0 букв називають пустим і позначають як .

Озн.5. Довжина слова – це є кількість букв в ньому, при чому однакові букви рахуються стільки раз, скільки вони входять в слово.

Озн.6. Множину всіх слів над алфавітом *A* позначають як множину *A\**.

Озн.7. Підмножини множини *A\** називають *мовами* над алфавітом *A*.

Приклади алфавітів

{а,б,в,г,...,ь,ю,я}

{\_,-//-}

- кільце лишків за модулем 33, буквами є від [0;32]

Коли говорять про криптосистему або шифр мають на увазі наступні об’єкти:

1. Простір повідомлень **A**

Тобто нехай маємо алфавіт A, в якому записується повідомлення або відкриті тексти. Відкрите повідомлення M є словом в цьому алфавіті, . Тобто множина A\* називається *простором повідомлень* або відкритих текстів.

1. Простір криптотекстів **B**

Тобто множина B\* називається простором криптотекстів і часто A=B

1. Простір ключів **K**

Складається із слів в деякому алфавіті, ці слова називають ключами.

1. Зашифровуюче відображення **E**

Простір відкритих текстів A\* за допомогою простору ключів відображається в простір шифротекстів

1. D:
2. Відображення E і D повинні мати наступну властивість – можливість розшифрування інформації: ,

# Класичні криптосистеми та їх криптоаналіз

## Шифри простої заміни

Перетворюють відкритий текст таким чином, що кожен його символ заміняється на якийсь інший символ, при цьому однаковим символам у відкритому тексті відповідають однакові символи у шифр-тексті. Ключем шифру простої заміни є таблиця підстановок, яка вказує в який саме символ криптотексту переходить кожен символ відкритого тексту.

Прикладом може бути шифр Цезаря, де шифром є звуження тексту. Алфавіт шифр-тексту в шифрі простої заміни не змінює суті тексту і його стійкості. Тому далі вважаємо, що відкриті тексті і шифр тексту записуємо в однаковому алфавіту.

Кількість всіх можливих ключів в шифрі простої заміни для українського алфавіту дорівнює: 33, 32, 31, ..., 1 = 33!

Якщо в алфавіті n букв, то кількість ключів = n!

Простір ключів шифру зсуву є значно меншим і дорівнює *n-1* різних ключів.

На практиці для формування ключа часто використовували ключове слово. Такий шифр називають шифром Цезаря з ключовим словом. Ключовими параметрами такого шифру є число [0;n-1] і слово в даному алфавіті.

Приклад для українського алфавіту з числом і ключовим словом:

3, хешування хешуваня

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |  | 29 | 30 | 31 | 32 |
| а | б | В | г | ґ | д | е | є | ж | з | и | і | ї | Й | ... | Щ | ь | ю | Я |
| щ | ь | ю | **х** | **е** | **ш** | **у** | **в** | **а** | **н** | **я** | б | г | ґ |  | т | ф | ц | Ч |

Простір ключів є обмеженим

## Криптоаналіз шифру прострої заміни

Через величину шифру простої заміни брутальна атака на такий шифр є безперспективною. Але це не означає, що шифр в цілому є стійкий.

Шифр простої заміни легко ламається з допомогою методу, який був основою криптоаналізу, який був основою криптоаналізу до середини 20го століття. Цей метод називають частотним аналізом.

### Частотний криптоаналіз

Отже означення: ***частота символу*** в тексті дорівнює кількості його входжень у цей текст, поділеній на загальну кількість символів в тексті.

Наприклад, відкритий текст «криптологічні\_перетворення». Загальна кількість букв – 26. Частота букви о в цьому тексті – 3 рази/26 букв. Якщо взяти букву «і», то її частота 2/26.

Основою частотного криптоаналізу є такий емпіричний фактор: в досить довгих текстах кожна буква зустрічається в приблизно однаковою частотою, залежною від букви і незалежною від тексту. Спираючись на даний факт з кожним символом пов’язують деяке число – частоту деякого символу у мові. Таблиці частот для різних мов є відомі. За допомогою таких таблиць шифр простої заміни ламається дуже легко, оскільки в шифрі простої заміни кожна буква відкритого тексту завжди заміняється однаково. Зворотня заміна при частотному аналізі не завжди вірна. Тоді застосовують інший феномен людської мови – феномен надлишковості. Більше того, в кожній мові є група букв (8-9), які зустрічаються найчастіше і заповнюють близько ¾ текстів даної мови. Тому при частотному аналізі достатньо правильно встановити ці найбільш вживані букви і завдяки надлишковості текст повідомлення вже можна зрозуміти.

Криптоаналітики одночасно з частотним аналізом застосовують інші прийоми, які дозволяють спростити аналіз. Наприклад, якщо перед шифруванням з відкритого тексту не вилучені пропуски, криптоаналітик може достатньо легко встановити слова з одною-двох букв, яких в кожній мові є небагато, звичайним вгадуванням і перевіркою осмивленості. Застосовують також ***протяжку ймовірного слова***. Наприклад, криптоаналітик припускає, що це лист і шукає по «Шановний». Ці додаткові прийоми дозволяють спростити частотний аналіз і таким чином скоротити об’єм даних, необхідних для успішного аналізу.

Показано, що шифр простої заміни можна зламати, перехопивши шифр-текст, об’єм якого не менший за кількість букв в даному алфавіті.

Частотний аналіз дозволяє комп’ютеру відрізняти осмислений текст і цей факт дозволяє автоматизувати процедуру криптоаналізу інших шифрів (навіть стійких).

## Гомофонний шифр заміни

Шифр заміни стійкий до класичного однолітного частотного аналізу був винайдений Карлом Фрідріхом Гаусом. В цьому шифрі кожен симол відкритого тексту заміняється не єдиним символом, а будь-яким символом з деяких можливих. Вибір варіанту заміни щоразу здійснюється випадково. Обов’язкова умова – різні символи відкритого тексту мають замінятися символами шифр-тексту. Тобто множини цих замін не повинні пересікатися. Це означає, що алфавіт шифр-тексту більший за алфавіт відкритого тексту. Кількість варіантів заміни кожної букви пропорційна її частоті. Часто для заміни символів використовують числа.

Однолітерний частотний аналіз для такого шифру не дає результату, але результативним є інший варіант частотного аналізу – аналіз ***частотних біграм***.

2010-03-18

Лекція №4

# Поліграмні шифри

Послідовність кількох букв тексту називається поліграмою. Послідовність з двох букв називається біграмою або диграфом. З l-букв, l-грамою. 3,4 букви: три- і тетраграми.

Ідея поліграмних шифрів полягає у заміні не окремих символів відкритого тексту, а сукупності кількох символів або l-грами. Тобто відкритий текст при шифруванні розбивається на блоки (або l-грами) і кожна така l-грама заміняється на якийсь символ чи групу символів

## Шифр Playfair’а

Це є біграмний шифр. Розглянемо його на прикладі шифрування тексту латинкою. Для цього використовується квадрат 5х5, в якому записують всі букви латинського алфавіту, крім j(яка найрідше зустрічається).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| S | Y | D | W | Z |
| R | I | P | U | L |
| H | C | A | X | F |
| T | N | O | G | E |
| B | K | M | Q | V |

При шифруванні відкритий текст розбивається на біграми так, щоб вони не містили однакових букв. Якщо біграми містять їх, текст модифікується так, щоб не змінити зміст повідомлення.

Кожна біграма зашифровується за допомогою такого квадрату за двома наступними випадками:

1. *Якщо дві букви біграми не попадають в один рядок чи стовпчик квадрату*, тоді вони визначають прямокутник і заміняються буквами з протилежних вершин.

Наприклад, CE: C -> F, E ->N.

1. *Якщо дві букви біграми попадають*, тоді вони циклічно зсуваються на одну позицію вправо або вниз відповідно.

*Наприклад:* KV -> MB, IK -> CY

Ключем шифру є розсташування букв в квадраті. Для зручності застосовують ключове слово, яке, після вилучення букв, записували з верхнього лівого квадрату зверху вниз. Далі записували решту букв алфавіту.

Шифр Плейфейра розкривається аналізом частот біграм.

Поліграмні шифри з l = 2,3,4, подаються частотному аналізу бі-, три-, тетраграм.

## Поліалфавітні криптосистеми

Всі розглянуті раніше шифри були одноалфавітними. Тобто застосовувалась одна таблиця підстановок і завжди при шифруванні кожен символ чи група символів замінювались однаково, в не залежності від позиції цього символа у тексті.

Якщо для шифрування використовують різні таблиці підстановок, застосування яких визначається позицією букви в тексті, тоді такі шифри називають **поліалфавітними**. Одною з найдавніших криптосистем є *шифр Віженера*.

Шифр подібний до шифру Цезаря, в якому ключ змінюється від кроку до кроку. При шифруванні під відкритим текстом записують ключове слово, яке повторюють, при необхідності, потрібну кількість разів. Номер букви ключового слова в алфавіті визначає число позицій, на які буде зсунута відповідна буква відкритого тексту.

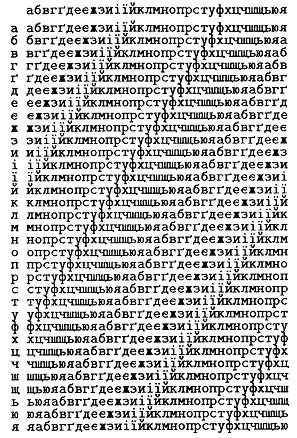
Відкритий текст: ПАРОЛЬАДЛЯАЛІСИДЛЯБОБАВ

Ключ: КЛЮЧ

|  |  |
| --- | --- |
| + | ПАРОЛЬАДЛЯАЛІСИДЛЯБОБАВ |
| КЛЮЧКЛЮЧКЛЮЧКЛЮЧКЛЮЧКЛЮ |
|  | АЛОЇЦЇЮЯЩКЮЗХГЖЯЩКЯЇЛЛА |

Позиція букви К-14, Л-15, Ю-31, Ч-27; тому букви, які опинилися над буквою К будуть зсунуті на 14 позицій, ... . В результаті отримаємо криптотекст.

Це все дуже важко, тому при шифруванні зручно користуватися таблицею Віженера



При шифруванні буква *відкритого тексту* визначає рядок, а буква *ключа* – стовпчик.

## Криптоаналіз шифру Віженера

Шифр Віженера може бути розкритий за допомогою частотного аналізу, якщо відома довжина ключа. Для цього криптотекст необхідно розбити на частини, кожна з яких шифрувалась своєю величиною зсуву. Спосіб визначення невідомого періоду запропонував в 60х роках XIX століття німецький криптоаналітик *Казізкі*. Він слідкував за появою в криптотексті однакових l-грам і вважав це ознакою наявності однакових l-грам у відкритому тексті, а також ознакою того, що відстань між ними кратна довжині періоду.

Визначивши відстань між однаковими l-грамами, в якості довжини ключа випробовують всі числа, які ділять цю відстань, для кожного числа здійснюють частотний криптоаналіз доки не доб’ються вірного результату.

## Шифр Віженера з автоключем

Шифрування здійснюється так само як у шифрі Віженера, але ключову послідовність формують інакше. Ключове слово пишемо раз, до нього дописуємо початковий відрізок відкритого тексту:

|  |  |
| --- | --- |
| + | ПАРОЛЬАДЛЯАЛІСИДЛЯБОБАВ |
| **КЛЮЧ**ПАРОЛЬАДЛЯАЛІСИДЛЯБ |
|  | АЛОЇБЬРУЬЩАРЦРИРЦРЇУМЯГ |

Шифр з автоключем також піддається криптоаналізу за методом Казіскі. За цим методом визначають довжину ключа, після чого ключове слово знаходять перебором.

В основі криптоаналізу є те, що деякі слова в кожній мові є частовживаними, тому можна сподіватися, що відстань між ними у досить довгому тексті, хоча б раз виявиться кратною періоду, а це приведе до появи l-грам в криптотексті, відстань між якими кратна довжині ключа.

Наприклад, в українській мові часто зустрічається слово **для**. Якщо відстань у відкритому тексті між двома такими словами не кратна довжині ключа, в криптотексті будуть різні l-грами. Але рівно між двома триграмами знаходиться слово, яке в ключі буде визначати нашу триграму



Якщо застосовується шифрування блоками (тобто відкритий текст розбивається на блоки по l символів в кожному), кожен з яких піддається шифруванню, то такі шифри називають блоковими з періодом l.

Шифр Віженера можна розглядати як блоковий шифр з періодом, що дорівнює ключовому слову.

## Шифри перестановки

Шифри перестановки зберігають всі букви тексту, розміщуючи їх в іншому порядку. Прикладами є шифр Скитала і шифр Загорожі. Такі шифри називають шифрами обходу

### Матричні шифри обходу

Повідомлення записують рядками у вигляді прямокутної таблиці. Криптотекст формується зчитування букв стовпчиками у послідовності, яка визначається ключем. Приклад:

Відкритий текст: ОХОРОНУСКЛАДІВПОСЛАБЛЕНО

Ключ: КЛЮЧ

1243

Далі записують відкритий текст рядками:

|  |  |  |  |
| --- | --- | --- | --- |
| К | Л | Ю | Ч |
| 1 | 2 | 4 | 3 |
| О | Х | О | Р |
| О | Н | У | С |
| К | Л | А | Д |
| І | В | П | О |
| С | Л | А | Б |
| Л | Е | Н | О |

і криптотекст отримуємо зі стовпчиків: ООКІСЛХНЛВЛЕРСДОБООУАПАН

Ключ як правило задавали у вигляді слова. Такий ключ у сучасному розвитку легко визначається за допомогою словникової атаки.

Загальний шифр перестановки з періодом l переставляє l букв у довільному порядку. Цей порядок визначається ключем. Ключ зручно задавати у вигляді таблиці

Таблиця показує, що перша буква блоку відкритого тексту займає позицію відкритого тексту і так далі.

При невеликому періоді l шифр перестановки легко розкривається спеціально організованим аналізом частот біграм. Приклад, який це демонстрірує:

Нехай перехоплено криптотекст:

ІЦКАЗИВИМЯИЛКИНОЙРЕСРПІНЗМЕЛБО

ПИРПИИТИНИИВІСВИТАЛП

Відомо, що він отриманий шифром перестановки з періодом 5. Його можна розшифрувати, розбивши на блоки по 5 букв і знайти правильне розміщення стовпчиків.

**12345**

ІЦКАЗ

ИВИМЯ

ИЛКИН

ОЙРЕС

РПІНЗ

МЕЛБО

ПИРПИ

ИТИНИ

ИВІСВ

ИТАЛП

Для того, щоб визначити правильний порядок стовпчиків можна використати інформацію про малі частоти біграм в українській мові.

Щоб у розшифрованому тексті не проявилася неможлива біграма ИИ, поряд не можуть стояти 1-3 стовпик, 1-4, 2-5, а також будь-які 2 з 1,3,5.

2010-03-22

Лекція №5

## Кількаразове шифрування

Алгоритм, який шифрує повідомлення одним шифром, а потім результат шифрування – ще одним шифром, називається ***композицією*** або добутком двох шифрів.

Відомо, що композиція матричних шифрів обходу призводить до перестановки, яку набагато важче завдати саму по собі. Відомо також, що при компонуванні двох блокових шифрів взаємнопростими періодами, період добутку шифрів збільшується.

Найвідоміший кількаразовий шифр періоду першої світової війни – це шифр з назвою ADFGVX. Цей шифр є композицією двох шифрів, підстановки та перестановки. Спочатку кожен символ відкритого тексту зашифровується шифром заміни, але заміняється не одним символом, а двома. Тобто застосовувалась так звана таблиці білітеральної підстановки подрібнення, а саме:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | A | D | F | G | V | X |
| A | C | O | 8 | X | F | 4 |
| D | H | K | 3 | A | Z | 9 |
| F | N | W | L | 0 | 7 | D |
| G | 5 | 8 | i | Y | H | U |
| V | 0 | 1 | V | B | 6 | R |
| X | E | Q | 7 | T | 2 | G |

В результаті отримували вдвічі довший криптотекст за відкритий текст(кожну букву або цифру цієї таблиці заміняли біграмою, перша буква якої позначала рядок, друга – стовпчик).

До проміжного криптотексту використовували звичайний матричний шифр обходу і отримували остаточний криптотекст.

Незважаючи на це шифр був взламаний французьким криптоаналітиком Жоржем Пенвелом.

## Роторні машини

В докомп’ютерні часи для автоматизації процесу шифрування застосовували різні механічні засоби. В основі конструкції більшості з них лежала концепція ротора – механічного колеса, що використовується для виконання підстановок.

Роторна машина складається з клавіатури і набором зв’язаних між собою роторів. Вона реалізує варіант шифру Віженера. На кожному роторі в довільному порядку розміщені букви алфавіту. Він має 26 фіксованих позицій і може виконувати просту підстановку. Взаємне розміщення роторів може змінюватися.

Найбільш відомий роторний пристрій – машина Енігма, застосовувалась Німеччиною в ІІ світовій війні. Вона мала 3 ротори, якщо вибирались з набору 5ти роторів. Крім того вона мала комутатор, який перетасовував відкритий текст, а також так званий відображаючий ротор, який заставляв кожен ротор двічі обробляти вхідний текст.

## Подання тексту в цифровій формі

В докомп’ютерні часи не було необхідності змінювати алфавіт відкритого тексту. Якщо існує необхідність скористатися сучасними засобами передачі даних, або перекласти шифрування на комп’ютер, виявиться, що звичайний алфавіт є незручною формою представлення, обробки і передачі інформації. Зручнішим є подання інформації в цифровій формі. Існують різні способи подання інформації в цифрі(способів первинного кодування).

В криптології найпростішим і достатньо розповсюдженим є спосіб, за яким кожна бува замінюється за її номером в алфавіті. Нумерацію, як правило, починають з нулика. Наприклад, слово «банан» можна представити як 0100170017. Номери букв можуть бути записані не в десятковій, а в двійковій системі числення. Всю послідовність бітів називають двійковим словом.

## Афінні шифри

Це підклас шифрів заміни, що включає часткові випадки шифр зсуву, Віженера, перестановки з фіксованим періодом, тощо.

*Зауваження!* Моноалфавітні *k*-гранні шифри заміни можна позначити як блокові шифри з періодом k. Відповідно шифр простої заміни можна трактувати як блоковий шифр з періодом 1.

*Правило!* *n-*символьний алфавіт ототожнюємо з кільцем Zn. Якщо в алфавіті 33 букви, то користуємся Z33, якщо латинська абетка – Z26.

Після прийняття такого правила до букв відкритого тексту можна застосовувати операції додавання і множення за відповідним модулем.

Отже n – кількість букв в алфавіті відкритого тексту.

## Шифри

### Шифр зсуву

Ключ: s,

Зашифрування: x

Кожна буква **x** відкритого тексту(мається на увазі номер букви) замінюється буквою **y**, .

Розшифрування:

### Лінійний шифр

Ключ: a 0<a<n НСД(a,n)=1

Зашифрування:

Розшифрування:

### Афінний шифр

Він є узагальненням шифром зсуву і лінійного шифру.

Ключ: a,s 0<a<n, , НСД(a,n)=1

Зашифрування:

Розшифрування:

### Афінні шифри вищих порядків

Розширемо розглянуті монограмні афінні шифри на шифрування *k*-грам.

Введемо операцію додавання – множина *векторів* – цифрових відображень k-грам в n-буквеному алфавіті.

Сумою векторів і , які належать є вектор X+S, що має такі координати:

Вектор є оберненим до S.

### Шифр зсуву kго порядку(шифр Віженера з періодом k).

Ключ:

Зашифрування: , кожна k-грама X замінюється Y, де

Розшифрування: ,

*,*

### Лінійний шифр kго порядку (криптосистема Хілла)

Хілл – це гора, Ванько поправив, що це пагорб.

- множина всіх можливих матриць /

Через позначаємо підмножину оборотніх матриць, яка об’єднує тільки ті матриці, до яких існують обернені.

Для деякої матриці A, яка належить визначаємо обернену до неї матрицю позначаємо ..

Добутком матриці на вектор стовпчикє вектор-стовпчик:

Зашифрування: Відкритий текст розбивається k-грамами,

Розшифр:

### Афінний шифр k-го порядку

Ключ: , НСД(w, n)=1

Зашифр.:

Розшифрування:

2010-03-24

Лекція №6

## Операція зсуву XOR

Застосовується в мобільному зв’язку, але зламати дуууже легко.

При *генеруванні* шифру відкритий текст піддається операції XOR побітово з ключем такої ж довжини. Якщо він коротший за повідомлення, то повторюється необхідну кількість разів.

*Розшифрування* здійснювання так само з тією самою ключовою послідовністю.

Криптоаналіз алгоритму XOR.

1. Визначають довжину ключа за допомогою процедури, яку називають *«підрахунок збігів»*. Для цього операцію XOR застосовують до шифртексту, використовуючи замість ключа сам шифртекст з різними зсувами;

Підраховують кількість байтів, які збігаються з байтами шифртексту(у випадку застосування ASCII кодування).

Якщо величина зміщення кратна довжині ключа, тоді збігаєтсья понад 6% байтів(*індекс збігу*). Якщо ні, тоді менше, ніж 0.4%. Мінімальне зміщення, яке дає високий індекс збігу і є довжиною ключа.

1. Після визначення довжини ключа криптоаналітик зміщує шифртекст на величину ключа і додають за модулем 2 до незміщеного криптотексту. Результатом є ліквідація ключа.
2. Для інших кодувань процедура дещо інша, а принцип розкриття аналогічний.

## Шифр одноразового блокноту (абсолютно стійкий шифр)

Якщо в алгоритмі XOR замість ключа у вигляді повтореного n раз ключового слово взяти випадкову послідовність бітів такої ж довжини, що і відкритий текст, то отримаємо варіант алгоритму одноразового блокноту.

Операцію зашифрування можна здійснювати і надсимвольною інформацією. В цьому випадку підсумовування здійснюється за модулем n(к-ть букв в алфавіті).

Зауваження! Якщо в шифрі Віженера в якості ключової послідовності вибрати строго випадкову послідовність букв, тої ж довжини, що і повідомлення, тоді також отримаємо шифр одноразового блокноту. Шифр винайдений в 1917 році Гілбертом Верномом і Мейджором Джозефом Моборном. Цей шифр абсолютно стійкий (в теоретико-інформаційному сенсі). Тобто його теоретично неможливо розкрити. Гарантією абсолютної стійкості, як показав Шеннон, є довжина ключа, його строга випадковість, а також однократність застосування.

Наприклад, назифруємо слово банан цим шифром.

Подаємо слово «банан» двійковим словом M

= 000001 000000 010001 000000 010001

Далі вибираємо випадковий двійковий ключ K такої ж довжини. Наприклад:

K = 001101 110101 100010 011000 111010

І додаємо:

C = 001100 110101 110011 011000 101011

Рано чи пізно криптоаналітик отримає слово «банан», але з ключем:

K’ = 001111 100001 100100 000100 101011

Він отримає відкриту послідовність, яка означатиме «груша». Це і є поняттям стійкості.

Недоліком шифру одноразового блокноту є складність процедури обміну ключем. Ключ довгий, таємний і повинен використовуватися лише 1 раз. Відповідно повинен бути таємний канал. Іншим недоліком є необхідність синхронізації прийому та передачі. Якщо приймач втратить хоча б 1 біт шифртексту він не зможе розшифрувати текст. Також він не забезпечує захист даних від спотворення.

Не дивлячись на ці недоліки, абсолютна стійкість є надзвичайним плюсом.

## Потокові шифри

Бінарний варіант шифру одноразового призначення відноситься сюди.

Озн. Потоковим називається шифр, який двійкове повідомлення (яке складається з i-тих бітів повідомлення), з використанням двійкового ключа такої ж довжини перетворює в криптотекст шляхом побітового додавання M та K за модулем 2.

Різновиди потокових шифрів відрізняються способом формування ключа.

Через складність процедур генерування та обміну випадкових таємних великих чисел на практиці в якості ключа застосовують псевдовипадкові числа.

Ключову послідовністю потокових шифрів називають γ-послідовністю, а потокове шифрування часто називають *гамування*.

Озн. Генератор псевдовипадкових бітів – це пристрій або алгоритм, який за заданими параметрапи продукує послідовність бітів, при чому значення кожного чергового iтого біта, не знаючи параметра, неможливо передбачити з ймовірністю, більше, ніж 0.5. Знаючи параметри значення чергового біта можна передбачити з ймовірністю 1.

Таємним параметром як правило є справжнє випадкове число, меншої за необхідну довжину. Це число часто називають парустком, який породжує гаму. Стійкість повністю залежить від надійності та граду криптоключа.

## Алгоритм DES

Процес прийняття DES і сам DES, так само як і роботи Шеннона, так само як і поняття абсолютно стійкого шифру склали основу сучасної криптографії.

NBS ініціювало в 1972 розробку єдиного стандарту крипто-алгоритму. Такий алгоритм можна було сертифікувати, а різні криптографічні засоби на його основі могли б взаємодіяти між собою.

Алгоритм міг бути відносно недорогим та доступним.

В 1973 році, NBS опублікувало вимоги до алгоритму, який міг би бути прийнятий за стандартом:

1. Високий рівень захисту
2. Детальний опис і зрозумілість алгоритму
3. Надійність алгоритму спирається на ключ, а не на секретність алгоритму
4. Доступність всім користувачам.
5. Адаптованість до різних застосувань
6. Економічна вигідність апаратної реалізації
7. Ефективність застосування(швидкодія)
8. Можливість перевірки
9. Алгоритм дозволений для експорту.

В 1974 році була повторна пропозиція

Претендентом на стандарт став алгоритм Люцифе, запатентована розробка IBM. NBS та IBM провели переговори і домовилися про надання NBS невийняткової безкоштовної ліцензії на виробництво засобів на основі цього алгоритму. NBS звернулася до ANB за підвердженням стійкості. Воно підвердило стійкість, але поміняло таблиці підстановок.

ANB дозволило відкриту публікацію алгоритму, це є ключовим, оскільки цього раніше не було. В 1975 році алгоритм було опубліковано. В 1976 р., затверджено як стандарт для несекретних урядових каналів зв’язку. В 1981р., DES затверджений як стандарт для приватного сектору.

В 1983, -87, -92х роках DES перезатверджено як стандарт.

В 2001 році прийнято новий стандарт AES.

2010-04-01 (15 квітня буде модуль)

Лекція №7

# Тема: Опис алгоритму DES

На спрощеному рівні опису, **DES** – це комбінація двох стародавніх методів шифрування: підстановки та перестановки. DES є блоковим симетричним шифром, що шифрує дані 64бітними блоками. Ключем також э 64бітне число, але в ньому кожен 8-й біт для контролю парності. Тому *фак*тична довжина ключа DES – 56 біт. Рівень стійкості DES повністю залежить від ключа. Деякі ключі є слабими, але їх можна легко уникнути. Особлива комбінація алгоритмів підстановки та перестановки є складовою частиною DES. Таку складову частиину називають *раундом*.

DES складається з 16ти раундів. Одна і та сама комбінація методів застосовується до відкритого тексту і криптотексту 16 разів і тоді на виході маємо текст з шифробуками.

## Загальна структура DES



*K16 – 16-й раунд.*

*Один раунд відображає петлю Фестля.*

*Те, що частинки тексту переставляються, то перевагою буде те, що можна змінити порядок і розшифрувати. Недоліком є те, що обробляється тільки одна половинка за раунд. Для стійкості потрібно достатню кількість раундів.*

В алгоритмі DES застосовується тільки стандартна арифметика, логічні операції над окремими бітами та 64-бітними числами.

## Початкова і завершальна перестановки

Початкова перестановка 64-бітного блоку відкритого тексту не покращує стійкість DES. Наявність цієї перестановки DES пояснюється способом вводу інформації в мікросхему DES.

***Таблиця початкової перестановки:*** 58,50,42,34,... - *це біти які ставали на позиції.*

Завершальна перестановка обернена до початкової

***Таблиця завершальної перестановки:*** 40,8,48,16,...

## Схема одного раунду DES

hl

## Перетворення ключика

### Початкова перестановка ключика

*[викладач повільними рухами витирає дошку, рухаючись праворуч і ступаючи елегантсько то на каблук то на носочок свого мешта]*

Біти головного ключа DES також підлягають початковій перестановці. Перед цим з головного ключа вилучаються біти контрою парності(8й біт кожного байту ключа: 8,16,24,32,40,48,56,64).

Далі 56 біт, що залишилися, переставляються. Перестановка також пояснюється способом вводу інформації в мікросхему DES.

Таблиця початкової перестановки ключа: 57,49,41,... [перексерите си таблічьку]. Після перестановки ключ також умовно ділиться на ліву та праву половинку, які прийнято позначати відповідно C0 I D0.

Далі в алгоритмі DES генеруються 16 48бітових підключів раундів. Ці підключі Ki визначаються наступним чином: спочатку вилучаються біти контролю парності, потім переставляються і діляться на 2 половинки. Маючи вже визначеними будуємо для n-ного раунду одним або двома лівими зсувами з відповідно до наступної таблиці.

### Таблиця величин зсуву ключа

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Ki | | | | | | | | | | | | | | | | |
| Раунд | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| Величина зсуву | **1** | **1** | 2 | 2 | 2 | 2 | 2 | 2 | **1** | 2 | 2 | 2 | 2 | 2 | 2 | **1** |

Після цього вибирається 48 з 56 біт. Ці 48 біт переставляються. Така операція називається ***стискаючою перестановкою*** або ***перестановочною вибіркою***. 48бітний результат стискаючої перестановки і є раундовим підключем.

Таблиця стискаючої перестановки: 14, 17, 11, 24...

Завдяки зсуву для генерування підключа кожного раунду використовується інша підмножина бітів головного ключа.

### Розширююча перестановка

Застосовується на кожному раунді до правої 32 бітної половини 64 бітного результату попереднього раунду. Ця операція розширює праву половину даних Ri з 32 до 48 біт, при цьому біти переставляються.

Операція вирішує 2 завдання:

1. Приводить розмір правої половини даних , у відповідність з розміром підключа раунду для виконання операції XOR.
2. Викликає так званий лавинний ефект. Суть його в тому, що мала зміна відкритого тексту або ключа призводить до значних змін шифртексту.

Розширююча перестановка (aka E-блок) задається такою схемою(показано перестановку половини з 32 біт).



Табличко: 32, 1, 2, 3, 4...

### Підстановка в S-блоках

Підстановка (заміна) здійснюється за допомогою 8ми блоків підстановки(S-блоків). Кожен такий блок має 6бітовий вхід, 4бітовий вихід. Всы 8 блоків – різні.

При виконанні підстановки 48 вхідних біт діляться на 8м 6бітових блоків. Кожен такий блок обробляється своїм S-блоком – підставляється в 4бітовий блок.

### Схема включення S-блоків



Нумерація починається з 0. В таблиці певним чином перемішані 4бітні числа. 6 вхідних визначають номера рядка і стовпця, на перетині яких зчитується 4бітне число. Відбувається це так: нехай маємо 6 вхідних бітів S-блоку . Крайні біті об’єднюються і визначають двійковий номер рядка S-блоку.

4 середні біти визначають номер стовпця: (число від 0 до 15).

Таблиці підстановок S-блоків є такими:

S-блок 1: 14, 4,...

### Підстановка за допомогою S-блоків. Ключовий крок алгоритму DES.

Саме ця підстановка визначає стійкість DES, всі інші операції легко піддаються аналізу.

Результат підстановки, 32бітовий блок, поступає на вхід блоку перестановки в **P**-блоці, в якому здійснюється пряма перестановка 32-біт.

Таблиця перестановки в P-блоці: 16, 7, 20, … [пере*ерить*]

Далі результат перестановки підсумовується побітово за модулем 2 з лівою половиною вхідного 64бітного блоку даних. Далі ліва і права половина міняються місцями і починається наступний раунд.

Розшифрування в DES – самостійно ☺.