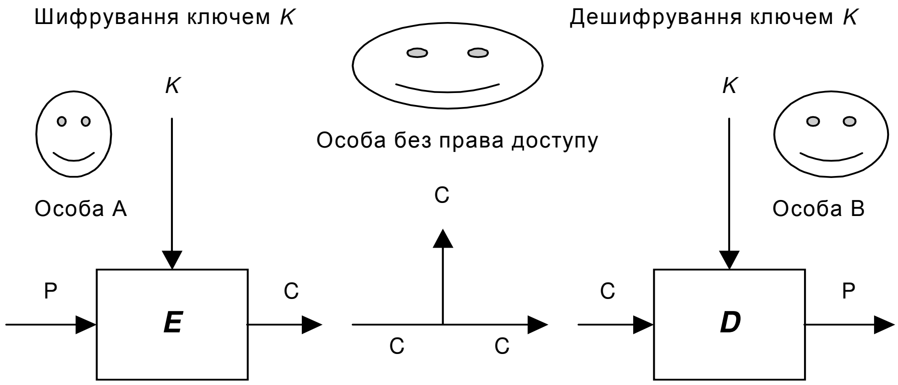
## *Лекція 20. Криптографічні застосування.*

З огляду на використання ключів розрізняють два методи шифрування: метод, що використовує симетричні алгоритми, та метод, що використовує асиметричні алгоритми.

*Симетричні алгоритми,* або алгоритми з *таємним* чи *приватним ключем* – це алгоритми, де ключ для шифрування та ключ для дешифрування є одним і тим самим.




Симетрична схема шифрування й дешифрування.

Симетричні алгоритми можуть бути потоковими або блоковими. Найвідомішим прикладом симетричного потокового алгоритму є шифр одноразового блокнота.

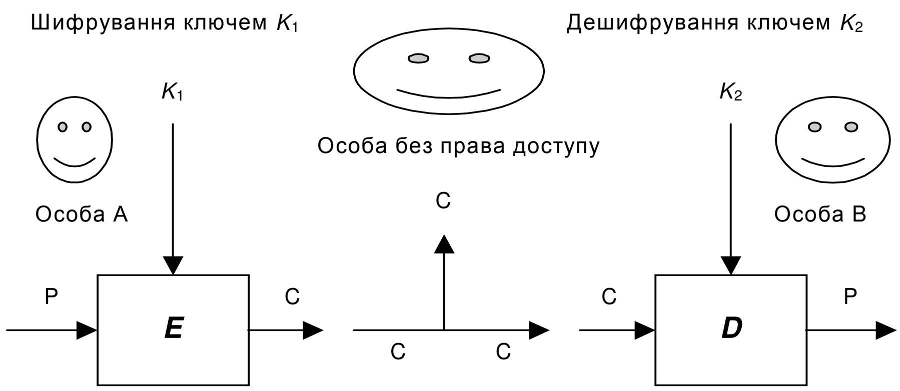
Якщо є дві послідовності бітів $A = a_1 \ldots a_k$, $B = b_1 \ldots b_k$, то під $A \oplus B$ розуміємо послідовність $C = c_1 \ldots c_k$, отриману виконанням операції додавання за модулем 2 над відповідними бітами обох послідовностей : $c_1 = a_1 \oplus b_1, \ldots, c_k = a_k \oplus b_k : C = A \oplus B$. У цьому разі $A \oplus 0 = A$ і $A \oplus A = 0$.

Припустимо, що явний текст є послідовністю бітів $M$, а ключ - послідовністю бітів $K$. Тоді криптограмою $C$ є послідовність бітів $C = M \oplus K$. Дешифрування ґрунтується на рівності

$$C \oplus K = (M \oplus K) \oplus K = M \oplus (K \oplus K) = M \oplus 0 = M.$$

*Асиметричні алгоритми,* або алгоритми з *явним* чи *публічним ключем* – це алгоритми, де ключі для шифрування й дешифрування різні.

у




Асиметрична схема шифрування й дешифрування.

Далі йдеться про застосування скінченних полів у криптографічному захисті інформації.

На початку 1997 р. фірма RSA Data Security оголосила конкурс на розкриття алгоритму блокового симетричного шифрування DES із довжиною ключа у 56 бітів. Його розкрили через 140 днів після початку конкурсу (протестовано 25% можливих ключів). Це засвідчило, що стандарт DES є далеко не оптимальним вибором для забезпечення таємності даних.

Тому Національний інститут стандартів США (NIST) у вересні 1997 р оголосив конкурс на створення нового американського стандарту шифрування, який повинен був замінити *DES*. Йому присвоєно робочу назву *AES* (Advanced Encryption Standard – удосконалений стандарт шифрування).

Переможцем конкурсу став алгоритм шифрування, запропонований Д. Даеменом та В. Рійменом. Алгоритм також називають *Rijndael,* ця назва утворена з початкових букв прізвищ авторів. Алгоритм *AES* затверджений як стандарт 2001 р.

Низку операцій в алгоритмі симетричного блокового перетворення *AES* визначено над байтами, які відображають елементи скінченного поля з 256 елементів (таке поле прийнято позначати $GF(2^8)$; варіант його побудови описано в лекції 18). Зокрема, перше з двох перетворень першого з чотирьох етапів циклу шифрування полягає в такому.

Спочатку байт розглядають як елемент поля $GF(2^8)$, що детально описано раніше. Якщо він ненульовий, то до нього відшукують обернений щодо множення в полі $GF(2^8)$. Якщо ж байт є нульовим, то для нього оберненого щодо множення не існує. Тому нульовому байту 00 відповідатиме він сам.

Інші операції визначено в термінах 4-байтових слів.

В Україні використовують аналогічний до *AES* шифр «Калина» (англ. *Kalyna*) – блоковий симетричний шифр описаний у національному стандарті України ДСТУ 7624:2014 «Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення». Стандарт набрав чинності з 1 липня 2015 року наказом Мінекономрозвитку від 2 грудня 2014 року №1484. Використано скінченне поле $GF(2^8)$ з іншим, ніж в $AES$, многочленом, який задає розширення

$$f(x) = x^8 + x^4 + x^3 + x^2 + 1.$$

Застосування елементів великого порядку в криптографії ґрунтується на так званій задачі дискретного логарифмування в будь-якій скінченній циклічній групі.

Нехай $G$ скінченна циклічна група, яка має $q$ елементів, з твірним елементом $g$. Використовуючи послідовні піднесення до квадрату, можна швидко (за поліноміальний час) обчислити $Y = g^X$ для будь-якого додатного цілого числа $1 \le X \le q-1$. Вважається, що маючи якийсь $Y$ обчислювально складно знайти дискретний логарифм від нього за основою $g$, тобто число $X$. Іншими словами, функція $f(X) = g^X$ є однонапрямленою. Проте, доведення цього на сьогодні немає.

Виходячи із задачі дискретного логарифмування переважно розглядають такі дві криптографічні схеми.

1) Протокол Діффі-Хелмана

Як можуть два користувачі узгодити таємний ключ (можливо, для криптосистеми з таємним ключем) через відкритий канал зв’язку ?

Користувачі погоджують $G$ скінченну циклічну групу, яка має $q$ елементів, та її твірний елемент $g$. Як $G$, так і $g$, є відкритими.

Користувач *A*: вибирає випадкове число $1 \le a \le q-1$, обчислює $g^a$ та пересилає значення $g^a$ користувачу *B*.

Користувач *B*: вибирає випадкове число $1 \le b \le q-1$, обчислює $g^b$ та пересилає значення $g^b$ користувачу *A*.

Користувач *A* обчислює $(g^b)^a$.

Користувач *B* обчислює $(g^a)^b$.

Тепер як користувач *A*, так і користувач *B* мають елемент групи $G$ рівний $g^{ab}$, який може слугувати як узгоджений таємний ключ.

2) Криптосистема Ель-Гамаля (криптосистема з відкритим ключем)

Нехай $G$ скінченна циклічна група, яка має $q$ елементів, з твірним елементом $g$. Як $G$, так і $g$, є відкритими.

Кожен користувач *U*: вибирає випадкове число $1 \le a \le q-1$ - секретний ключ для дешифрування. Тоді обчислює $g^a$ і виставляє його – це публічний ключ цього користувача..

Щоб переслати таємне повідомлення *P* користувачу *U*: слід вибрати випадкове число $k$, тоді обчислити та переслати пару значень $\beta_1 = g^k, \beta_2 = P(g^a)^k$.

Користувач *U* виконує дешифрування згідно з таким виразом $P = \beta_2(\beta_1)^{-a}$.

Зауважимо, що не обов'язково $g$ мусить бути твірним елементом групи $G$. Перша та друга описані криптографічні схеми працюють для будь-якого випадкового елемента $g$. Разом з тим їх стійкість до зламування залежить від мультиплікативного порядку елемента $g$. Цей порядок елемента у вибраній скінченній циклічній групі мусить бути достатньо великим.

У криптографії можливе застосування як групи $G$ таких скінченних циклічних груп:

1) Мультиплікативна група $Z_p^* = \{0,1,\dots,p-1\}$ відносно множення за модулем великого простого числа $p$.

2) Мультиплікативна група скінченного поля $F_{q^n}^*$

Питання побудови елементів великого мультиплікативного порядку розглядають як для загальних, так і для спеціальних скінченних полів. Для часткових випадків скінченних полів можна збудувати елементи, що мають набагато більші порядки. Огляд отриманих у цій області результатів станом на початок 2012 року наведений у розділі 4.4 (розділ написаний J.F.Voloch) довідника G. Mullen, D. Panario, Handbook of Finite Fields, 2013, CRC Press.

3) Еліптична крива $E(F_q)$ над скінченним полем $F_q$, яку описано в лекції 19.

Нагадуємо, що її переважно записують не в мультиплікативній, а в адитивній формі. Приклад еліптичної кривої, рекомендованої Національним інститутом стандартів США, наведено далі.

y

Draft NIST SP 800-186, Recomm

nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-186-draft.pdf

Draft NIST SP 800-186, Recommendation for Discrete Logarithm-Based Cryptography: Elliptic Curv... 25 / 78

#### 4.2.1.5 P-521

The elliptic curve P-521 is a Weierstrass curve $W_{a,b}$ defined over the prime field GF($p$) that has order $h \cdot n$, where $h$=1 and where $n$ is a prime number. This curve has domain parameters $D$=( $p$, $h$, $n$, *Type*, $a$, $b$, $G$, {*Seed*, $c$}), where the *Type* is "Weierstrass curve" and the other parameters are defined as follows:

*p*: $2^{521} - 1$

= 686479766013060971498190079908139321726943530014330540939\
446345918554318339765605212255964066145455497729631139148 \
0858037121987999716643812574028291115057151

(=`0x1ff ffffffff ffffffff ffffffff ffffffff ffffffff ffffffff ffffffff ffffffff ffffffff ffffffff ffffffff ffffffff ffffffff ffffffff ffffffff ffffffff`)

*h*: 1

*n*: 686479766013060971498190079908139321726943530014330540939\
446345918554318339765539424505774633321719753296399637136\
3321113864768612440380340372808892707005449

UK 20:12 03.12.2020