Лк №1
07.02.09

Лисицкая Ирина Викторовна

Защита информации в компьютерных сетях

Литература:

1. Горбенко І.Д. Криптографічний захист інформації. Навч. пос: Харків, ХНУРЕ. 2004г.
2. Вербицький О.В. Вступ до криптології. - Львів, 1998р - 247с.

информация - совокупность данных и программ, функционирующих в системе.

защита информации - совокупность организационно-технических мероприятий, правовых и морально-этических норм, административных мер, физических и программно-технических средств, направленных на противодействие угрозам автоматизированной системы обработки информации (АСОИ) или сведению к минимуму возможности ущерба.

доступ к информации - это ознакомление с информацией, ее обработка, копирование и уничтожение.

санкционированный доступ - доступ, не нарушающий правила разграничения доступа в системе.

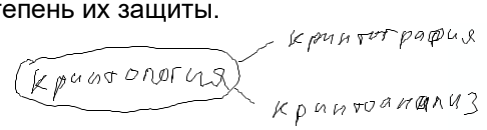
несанкционированный доступ - доступ, нарушающий правила разграничения доступа в системе.

правила разграничения доступа служат для регламентации права доступа субъектов доступа к объектам доступа.

субъект - активный компонент системы, который может стать причиной потока информации от объекта к субъекту, или причиной изменения состояния системы.

объект - пассивный компонент системы, хранящий, принимающий или передающий информацию.

конфиденциальность данных - статус, предоставляемый данным, который определяет требуемую степень их защиты.



все системы существования делятся на два класса - симметричные криптосистемы и несимметричные. несимметричные также называются "двухключевые системы" или "системы с открытым ключом".

если система симметричная, то ключ шифрования равен ключу расшифрования. в несимметричных - не равен.

пример для алгоритма RSA:

1. абонент выбирает два больших простых числа P и Q.
2. считается N=P*Q - это модуль
3. рассчитывается функция Эйлера φ(N)=(P-1)(Q-1)
4. E - открытый ключ. $1 < E \leqslant \varphi(N)$, НОД(E,φ(N))=1

D - секретный ключ

$$DE \equiv 1(mod\varphi(N))$$

M - откр. сообщ.

$$C = M^E(modN)$$

$$M = C^D(modN)$$

пример: P=7, Q=11
N=7*11=77
φ(N)=60
E=13

$$13D \equiv 1(mod\,60)$$

$$D = \frac{1}{13}(mod\,60)$$

$$D = \frac{1+60\alpha}{13}$$

- необходимо найти такое α, чтобы деление было целочисленным.

α=8, D=37.

зашифруем число 2 (которое, например, соответствует букве Б в тексте)

M=2

$$C = M^E (mod N) = 2^{13} (mod 77) = 30$$

$$M = C^D (mod N) = 30^{37} (mod 77) = (30^2)^{15} 30^2 \cdot 30^2 \cdot 30^2 \cdot 30 (mod 77) = 53^{15} 53 \cdot 53 \cdot 53 \cdot 30 (mod 77) =$$

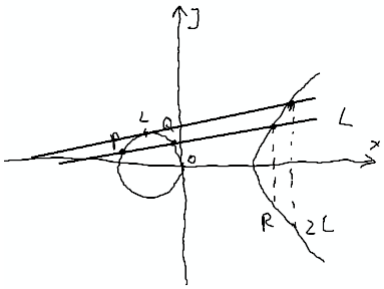
$$= (53^2)^6 \cdot 53^2 \cdot 53^2 \cdot 53^2 \cdot 30 (mod 77) = 37^6 \cdot 37 \cdot 37 \cdot 37 \cdot 30 (mod 77) = (37^2)^3 \cdot 37^2 \cdot 37 \cdot 30 (mod 77) = 2$$

система Эль-Гамаля

в ней используется задача дискретного логарифмирования: при известных Y, A, и N, найти такое X, чтобы выполнялось $Y = A^X (mod N)$

эллиптическая кривая

P(x_1,y_1)
Q(x_2,y_2)
R=P+Q=(x_3,y_3)
$P \neq Q$



афинная система подстановок Цезаря

$$E_{a,b} = at + b (mod m)$$

m=32 - используются 32
буквы русского алфавита без буквы ё.
1 < a,b < m
НОД(a,m)=1
a=17
b=25

$$E_{a,b} = 17t + 25 (mod 32)$$

А	0	25
Б	1	10
В	2	27
Г	3	12
Д	4	29
Е	5	14
Ж	6	31
З	7	16
И	8	1
Й	9	18
К	10	3
Л	11	20
М	12	5
Н	13	22
О	14	7
П	15	24
Р	16	9
С	17	26
Т	18	11
У	19	28
Ф	20	13
Х	21	30
Ц	22	15
Ч	23	0
Ш	24	17
Щ	25	2

Ь	26	19
Ы	27	4
Ъ	28	21
Э	29	6
Ю	30	23
Я	31	8

Лк №2
07.02.23

основные понятия и определения криптографии. простейшие шифры замены и перестановки

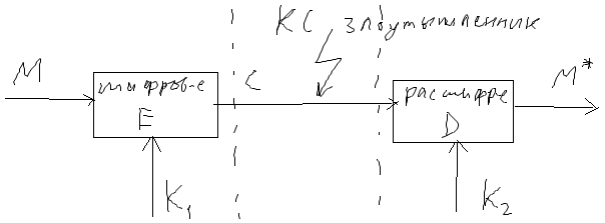
ключ - некоторая последовательность символов, управляющая процедурами шифрования/расшифрования.

шифрование - преобразование данных по закону ключа.

расшифрование - процедура, обратная шифрованию.

шифр-текст (криптограмма) - преобразованные данные с закрытым семантическим содержанием (семантический - "один в один")

классическая криптографическая схема защищенной передачи информации:



M - открытое сообщение (открытый текст)
C - криптограмма (шифр-текст)
K_1, K_2 - ключи
в идеале $M = M^*$, но т.к. в канале могут быть потери, шумы и т.п., это выполняется не всегда
E - процедура шифрования
D - процедура расшифрования
если $K_1 = K_2$, то это - симметричная система
если $K_1 \neq K_2$, то несимметричная
$C = E_{K_1}(M)$ - т.е. криптограмма C получается из открытого сообщения M с использованием процедуры шифрования E и ключа K_1
$M^* = D_{K_2}(C)$

к любым шифрам предъявляются как минимум два требования:
1. надежность
2. эффективность (процедуры должны выполняться достаточно быстро)

система подстановок Хилла
$Z_m \to Z_m$
$m = 26$
2,13
$det\begin{vmatrix} 3 & 3 \\ 2 & 5 \end{vmatrix} = 9$

$$\begin{vmatrix}3 & 3\\2 & 5\end{vmatrix}\begin{Vmatrix}a & b\\c & d\end{Vmatrix}mod m$$

$$\begin{cases}3a+3c(mod\,26)=1\\3b+3d(mod\,26)=0\\2a+5c(mod\,26)=0\\2b+5d(mod\,26)=1\end{cases}$$

$$3(a+c)(mod\,26)=1$$

$$a+c=\frac{1}{3}(mod\,26)$$

$$a+c=\frac{1+\alpha\cdot 26}{3}=9$$

$$2a+5(9-a)(mod\,26)=0$$

$$2a+45-5a(mod\,26)=0$$

$$45=3a(mod\,26)$$

$$a=15$$

$$c=9-a$$

$$c=9-15(mod\,26)=-6(mod\,16)=20$$

(ищем наименьшее положительное решение)

...

получаем, что обратная матрица (с помощью которой происходит расшифрование) -

$$\begin{vmatrix}15 & 17\\20 & 9\end{vmatrix}$$

PA YM OR EM ON EY

буквы английского алфавита нумеруются начиная с 0.

PA - 15 0

$$\begin{vmatrix}3 & 3\\2 & 5\end{vmatrix}\begin{Vmatrix}15\\0\end{Vmatrix}(mod\,26)=\begin{vmatrix}19\\4\end{vmatrix}\rightarrow TE$$

и т.д. - аналогично можно зашифровать остальные буквы.

$$TE\rightarrow\begin{vmatrix}15 & 17\\20 & 9\end{vmatrix}\begin{Vmatrix}19\\4\end{Vmatrix}(mod\,26)=\begin{vmatrix}15\\0\end{vmatrix}$$

можно делить текст и по три буквы (на *триграммы* вместо *биграмм*) - тогда матрица будет 3×3.

шифр считается одноалфавитным в широком смысле слова.

примеры многоалфавитных систем:

шифр Гронсфельда.

K=1348 (последовательность неповторяющихся цифр)

сообщение -

ПРИЕЗЖАЮВОСЬМОГО

подписываем ключ под сообщением -

1348134813481348

каждая буква сдвигается на соответствующее количество букв по алфавиту

еще одна многоалфавитная система - Веженера:

используется русский алфавит без буквы ё.

```
   АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЬЫЪЭЮЯ
0  АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЬЫЪЭЮЯ
1  БВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЬЫЪЭЮЯА
2  ВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЬЫЪЭЮЯАБ
3    . . .

ПРИЕЗЖАЮВОСЬМОГО
АМБРОЗИЯАМБРОЗИЯ
```

ПЪЙ...
(ключ - "амброзия")
- берется буква на пересечении соответствующих строки и столбца

трисемус

БАНДЕРОЛ
ЬВГЖЗИЙК
МПСТУФХЦ
ЧШЩЫЪЭЮЯ

- в таблицу последовательно вписываются буквы алфавита, не принадлежащие ключевому слову ("бандероль").

при шифровании берется очередная буква открытого текста и заменяется на букву, стоящую ниже в этой таблице. если буква - на последней строке, то она заменяется на букву из первой строки.

биграммный шифр плейфейр

для этого шифра таблица строится по той же идее, что таблица трисемуса. но идея шифрования другая. перед шифрованием сообщение разбивается на биграммы:

ПР ИЕ ЗЖ АЮ ВО СЬ МО ГО

берется первая биграмма, если ее две буквы не принадлежат одной строке или столбцу, то по ним строится прямоугольник и делается зеркальное отображение:
ФА ЗР ИЗ ...

"ЗЖ" - попали на одну строку. в этом случае - сдвиг на 1 вправо. если буквы в одном столбце, то сдвиг на один вниз (подобно шифру трисемуса).

двойной квадрат Уитстона

две таблицы со всеми буквами + знаки препинания:

ЖЩНЮР	ИУГЯТ
ИТЬЦБ	,ЖЬМО
ЯМЕ.С	ЗЮРВЩ
ВЫПЧ	Ц:ПЕЛ
:ДУОК	ЪАН.Х
ЗЭФГШ	ЭКСШД
ХА,ЛЪ	БФУЫ

ПР ИЕ ЗЖ АЮ _Ш ЕС ТО ГО
ПЕ ОВ ...

алгоритм DES

рассеивание - распростнанение влияния одного символа открытого текста на много цифр текста

перемешивание - использование таких шифрующих преобразований, которые затрудняют установление статистических свойств открытого и шифрованного текстов

алгоритм работает в нескольких режимах:

ECB
CBC (cypher block chaining) - сцепление блоков шифра
CFB - обратная связь по шифр-тексту
OFB (output feedback) - обратная связь по выходу

перед шифрованием открытое сообщение разбивается на блоки по 64 бита.

Лк №3
07.03.09

классические симметричные системы. ГОСТ 28147-89

это типичная классическая симметричная система. предусмотрено 4 режима работы:

1. режим простой замены
2. режим гаммирования
3. режим гаммирования с обратной связью

4. режим выработки имитовставки

для этой системы характерны дополнительные операции, которых не было в DES:

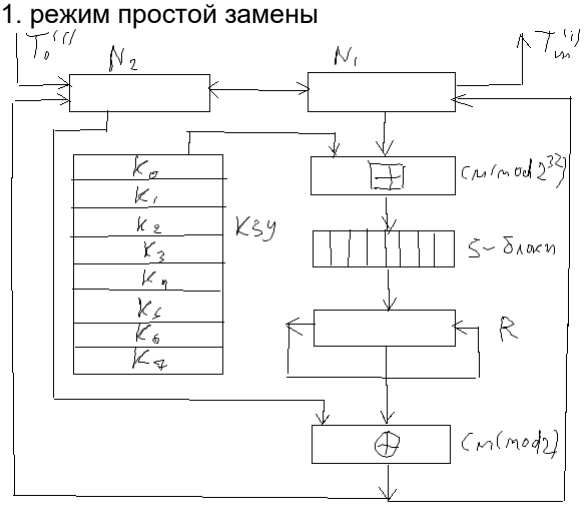
$\oplus$ - сложение по модулю 2

$\boxplus$ - сложение по модулю 2^{32}

$\boxplus'$ - сложение по модулю $2^{32}-1$

$$\begin{cases} a \boxplus b = a + b, & |a+b| < 2^{32} \\ a \boxplus b = a + b - 2^{32}, & |a+b| \geqslant 2^{32} \end{cases}$$

1. режим простой замены



2. режим гаммирования.

перед шифрованием в КЗУ вносят 256 бит ключа, причем сначала в N_1, N_2 вносятся не исходные данные, а некоторые случайные данные, синхропосылка, которая как обычно проходит 32 итерации в прежнем блоке. после чего данные суммируются с константами: левая часть по модулю 2^{32} с C_1, правая - по модулю $2^{32}-1$ с C_2. получили первый блок гамма-шифра...

3. режим гаммирования с обратной связью

4. режим выработки имитовставки

имитовставка - это блок из p бит, который вырабатывается по закону ключа и передается вместе с открытыми или зашифрованными данными, для обеспечения имитозащиты.

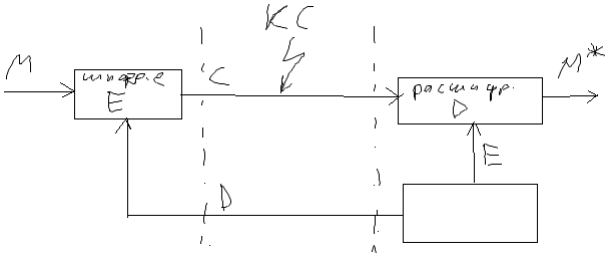
имитозащита - защита от навязывания ложных данных.

открытое сообщение разбивается как всегда на блоки в 64 бита. первый блок проходит 16 циклов в режиме простой замены, после этого результат складывается по модулю 2 со вторым блоком открытых данных, и опять проходит 16 циклов, складывается с третьим блоком... так весь текст обрабатывается до конца. из выходных данных берутся 32 бита, которые и будут имитовставкой.

Лк №4
07.03.23

концепция криптосистем с открытым ключом

основное отличие - что ключ шифрования не равен ключу дешифрования.



E - секретный ключ; D - открытый ключ.

Диффи и Хеллман сформулировали ряд требований, выполение которых необходимо для обеспечения стойкости криптосистем:

1. отправитель, зная открытый ключ D и открытое сообщение M, легко вычисляет криптограмму.

$C = E_D(M)$

2. получатель, зная секретный ключ E и криптограмму C, легко восстанавливает сообщение.

3. криптоаналитик, зная открытый ключ, при попытке вычислить секретный ключ, наталкивается на непреодолимые вычислительные сложности

4. криптоаналитик, зная открытый ключ D и криптограмму C, при попытке вычислить открытое сообщение M также наталкивается на непреодолимые вычислительные сложности.

криптосистема RSA

(авторы - Райлест, Шамир, Адлеман?..). в основе криптографической стойкости этой системы лежит задача факторизации, т.е. трудности разложения большого числа на множители.

N=P*Q

основа алгоритма:

1. выбираются два больших простых числа, лучше - сильные простые (т.е. само число N простое, и при этом N+1 имеет в своем разложении большой простой сомножитель; N-1 имеет в своем разложении большой простой сомножитель) P, Q.

2. N=P*Q - модуль

3. считается функция Эйлера - $\varphi(N) = (P-1)(Q-1)$

4. D - откр. ключ

$1 < D \leqslant \varphi(N)$, НОД$(D, \varphi(N)) = 1$

5. $E * D \equiv 1(mod\varphi(N))$

теорема Эйлера:

если НОД(x,N)=1, то $x^{\varphi(N)} \equiv 1(modN)$, или $x^{n\varphi(N)+1} \equiv x(modN)$

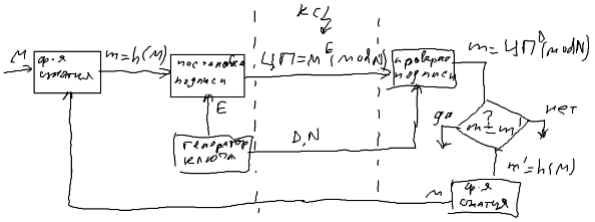
недостатки такого алгоритма: при выборе чисел P и Q приходится проверять большое количество дополнительных условий, что требует дополнительных затрат времени; также недостатком является то, что такая криптосистема подвержена мультипликативной атаке.

однонаправленные функции

некоторая функция, которая отображает множество $X \to Y$ является однонаправленной, если для любого $x \in X$ найдется такое $y \in Y$, что $y = f(x)$

зная целые A,N,y найти такое x, что $A^x(modN) = y$. если $A, N, y \sim 2^{664}$, то для решения такой задачи потребуется 10^{26} операций.

системы электронной цифровой подписи типа RSA:



5 видов злоумышленных действий, которые можно предотвратить использованием цифровой подписи:

1. активный перехват

2. "маскарад" - абонент C посылает абоненту B документ от имени абонента A.

3. ренегадство - абонент A заявляет, что не посылал сообщение абоненту B, хотя на самом деле посылал.

4. подмена. абонент B изменяет или формирует новый документ, и заявляет, что получил его от A.

5. повтор. абонент C повторяет ранее переданный документ, который абонент A когда-либо посылал абоненту B.

целью аутентификации является установление истинности и подлинности.

криптосистема Эль-Гамаля

это тоже двухключевая система. создана в 1985 году.