ЗАЩИТА ИНФОРМАЦИИ В СИСТЕМАХ ОБРАБОТКИ И ПЕРЕДАЧИ ДАННЫХ

ф-т ИКСС, гр. ИКВТ – 71,72; 4-ый семестр
Лекций – 7 (14 часов);
Лекторы: проф. Когновицкий О. С. (первые 3 лекции);
доц. Владимиров С. С. (4 следующие лекции).
Практические и лабораторные занятия – доц. Глухов А. Н.
Итоговый контроль- экзамен.

Литература.

1. Коржик В. И., Просихин В. П. Основы криптографии. Учебное пособие. – СПб: Изд. «Линк», 2008

Содержание лекций:

Лекция 1. Законодательные и нормативные документы по защите информации. Основные термины и определения. Обобщенные блок-схемы алгоритмов криптографических систем по защите информации. Простейшие криптографические системы защиты текстовой информации: подстановки (таблицы Виженера), перестановки, поточное и поблочное скремблирование.

Лекция 2. Поблочное шифрование с общим секретным ключом на основе ячеек Фейстеля. Американские стандарты шифрования DES и AES. Описание алгоритмов. Криптосистема с открытыми и закрытыми ключами. Стандарт RSA. Алгоритм работы. Алгоритм проверки целостности сообщения на основе хеш-функции.

Лекция 3. Алгоритм шифрования методом Эль-Гамаля. Алгоритм дистанционного формирования общего сеансового ключа по методу Диффи-Хеллмана. Протокол Шамира дистанционного определения общего секретного ключа.

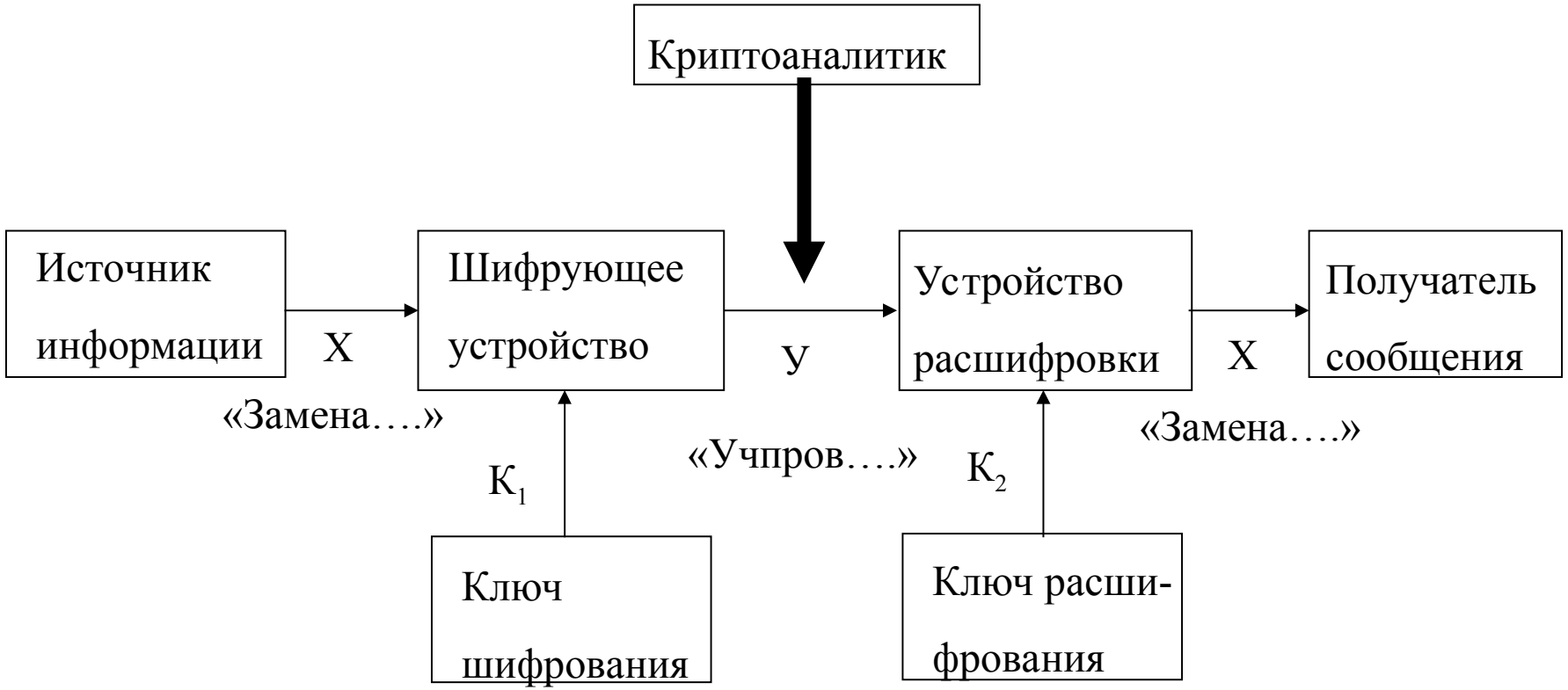
Лекция 4. Поточное и поблочное скремблирование. Алгоритмы. Принципы реализации.

Лекция 5. Шифрование файлов и электронных почтовых сообщений PGP.

Лекция 6. Международный стандарт сертификата открытых ключей X.509.

Лекция 7. Вопросы информационной безопасности в Интернет.

ОБЩАЯ БЛОК-СХЕМА СИСТЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ С КРИПТОЗАЩИТОЙ

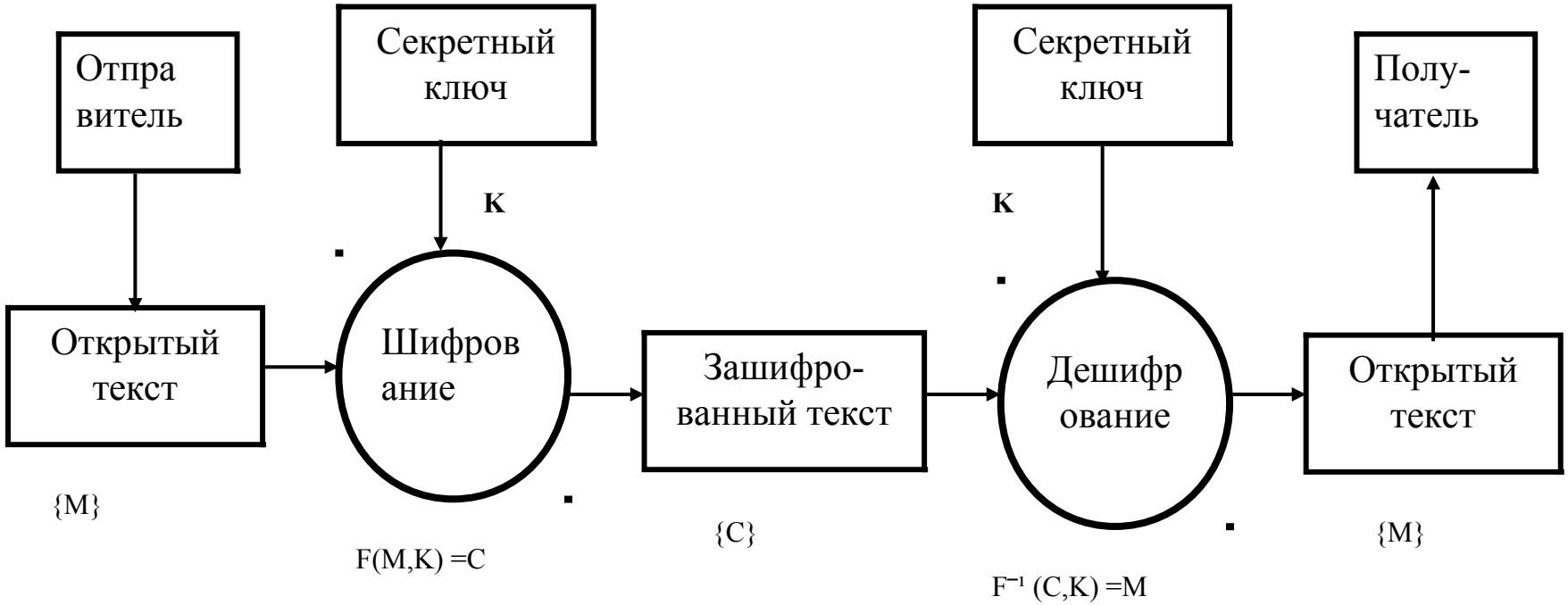


X – открытый текст

У – зашифрованный текст

Лекция 2. Поблочное шифрование с общим секретным ключом на основе ячеек Фейстеля. Американские стандарты шифрования DES и AES. Описание алгоритмов. Криптосистема с открытыми и закрытыми ключами. Стандарт RSA. Алгоритм работы. Алгоритм проверки целостности сообщения на основе хеш-функции.

1). Симметричные ключи (системы с общим секретным ключом).



M – открытый текст, подлежащий шифрованию;

C – зашифрованный текст;

K – общий секретный ключ шифрования;

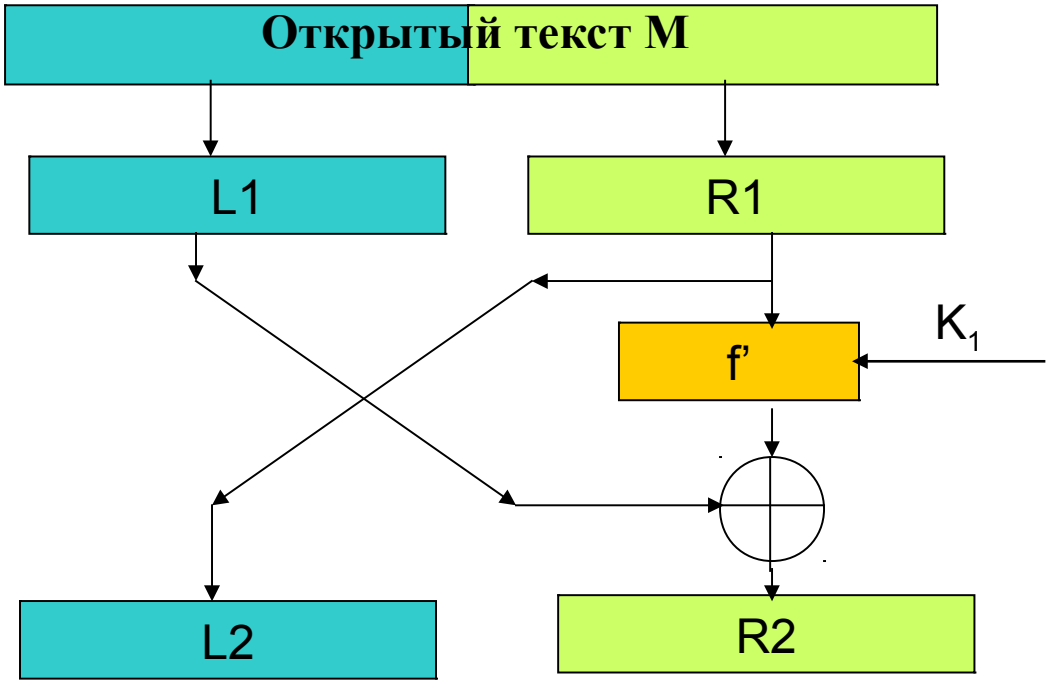
F(M,K) – функционал шифрования (криптографической защиты сообщения);

$F^{-1}(C,K)$ – обратный функционал расшифрования сообщения.

Пример: стандарт DES (Data Encryption Standard), США, принят в 1977 г.

Стандарт шифрования DES

- Ячейка Фейстеля:



$L_{i+1}=R_i$

$R_{i+1}=f'_k(R_i)+L_i \bmod 2$

Особенности шифрования ячейками Фейстеля:

- Обратимость шифрования;

- шифрование выполняется раундами, на каждом раунде выполняется одно и то же преобразование, но с разными ключами

Ячейки Фейстеля

- На последнем раунде (итерации) левая часть не меняется с правой.
- Расшифрование происходит по этой же схеме с обратным порядком раундовых ключей.
- Обычно для каждого раунда из основного ключа вырабатываются ключи итераций:
  - K -> (K_1,K_2,… , K_d) d- число итераций
- Проблема выбора размера блока
  - Большие блоки дают большую стойкость,
  - Маленькие блоки дают высокую скорость,

- Криптостойкость шифрования обычно повышается:
  - увеличением длин ключей;
  - увеличением числом итераций, от 16 до 32.

По схеме ячеек Фейстеля построено большинство шифров конца двадцатого века.

DES (Data Encryption Standard) – *Федеральный стандарт шифрования для несекретных сообщений в США*. Стандарт до 2000-го года.

Основан на структуре Файстеля

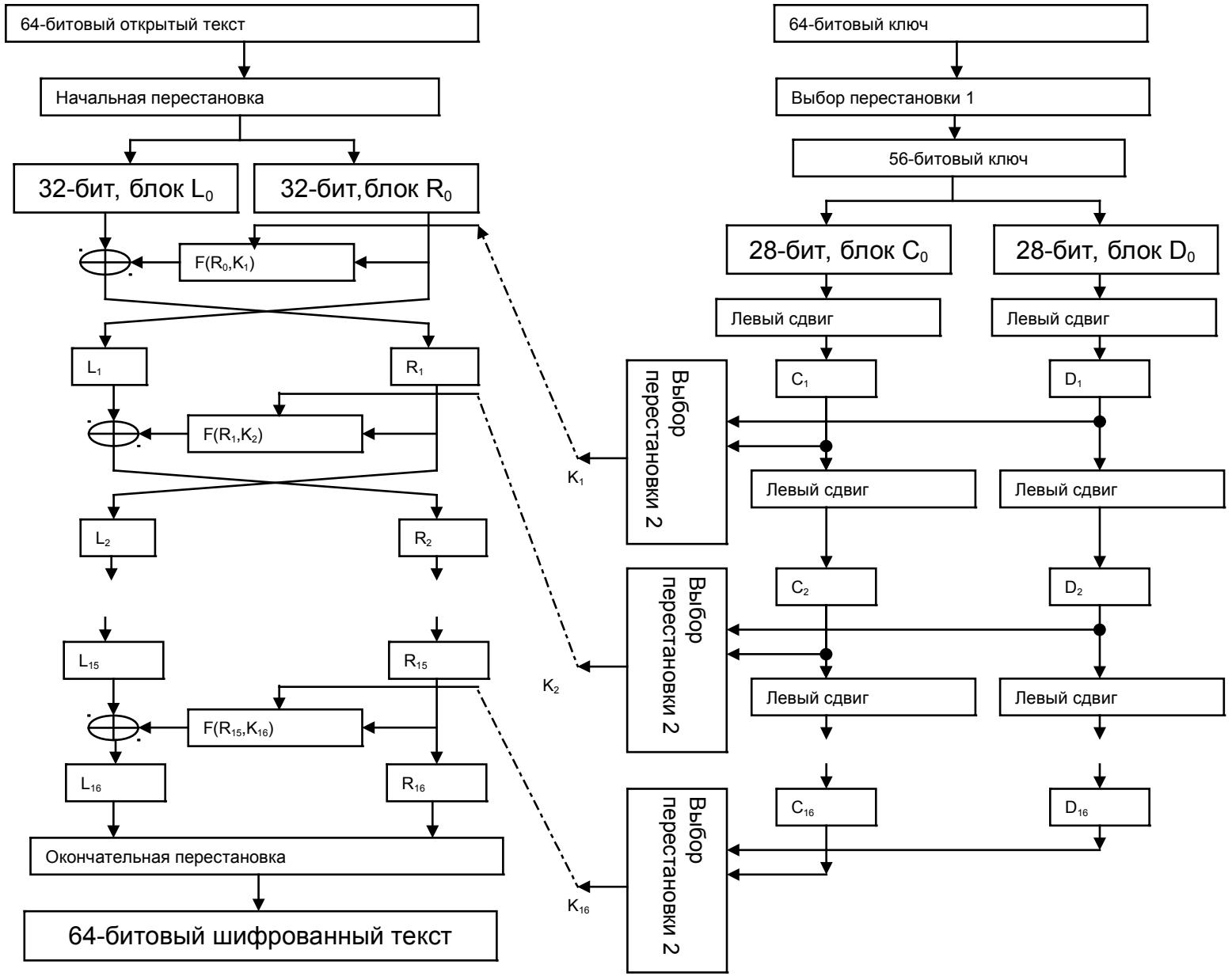
N=64=56 +8 проверочных – длина ключа

n=64 – длина блока

d=16 – число раундов (итераций)

Ключи итераций на основе циклического сдвига исходного ключа (на один или два разряда)

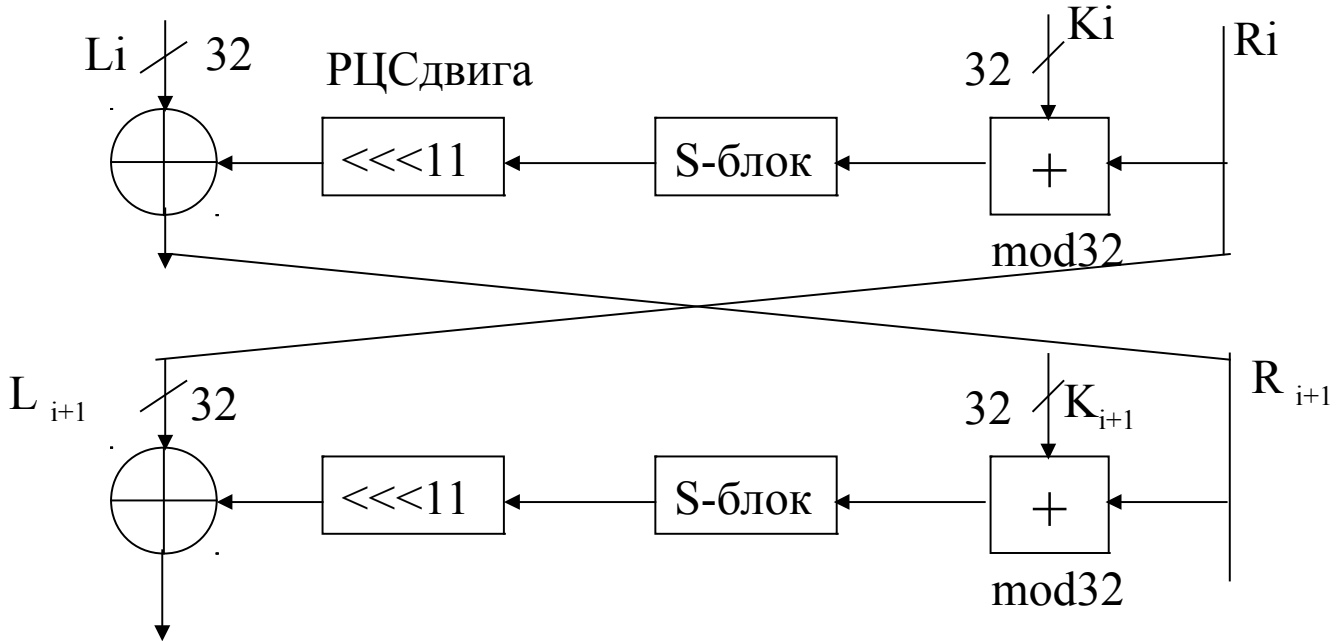
Стандарт шифрования DES (Data Enckryption Standard)



ГОСТ-28147-89

Государственный стандарт шифрования РФ.

- Основан на структуре Файстеля
- Длина ключа N=256 (Nдополн = 512)
- Длина блока n=64
- Число итераций d=32
- Ключи итераций на основе некоторой выборки бит из основного ключа.
- Повышение криптоустойчивости, по сравнению с DES, достигается использованием в нем, помимо табличных операций и операций по mod2, также операций по mod2^{32}.



AES стандарт в США с 2001 года

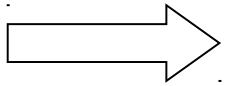
Advanced Encryption Standard

- Схема - квадрат из байтов,
  - Длины ключей N=128, 192, 256 бит
  - Длина блока данных n= 128,
  - d=f(N,n): d=10(N=128),12(N=192),14(N=256)

- Преимущества AES:
  - относительно высокая стойкость и скорость,
  - небольшая стоимость,
  - возможность эффективной программной и аппаратной реализации,
  - гибкость (переменная длина ключей)
  - реализуемость в системах с ограниченным количеством памяти.
- RIJNDAEL (Rijmen and Daemen) «Рейндолл»

1-ое преобразование

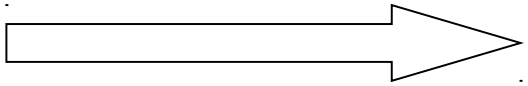
S_{00}	S_{01}	S_{02}	S_{03}
S_{10}	S_{11}	S_{12}	S_{13}
S_{20}	S_{21}	S_{22}	S_{23}
S_{30}	S_{31}	S_{32}	S_{33}



$$\begin{bmatrix} S_{00}^{-1} & S_{01}^{-1} & S_{02}^{-1} & S_{03}^{-1} \\ S_{10}^{-1} & S_{11}^{-1} & S_{12}^{-1} & S_{13}^{-1} \\ S_{20}^{-1} & S_{21}^{-1} & S_{22}^{-1} & S_{23}^{-1} \\ S_{30}^{-1} & S_{31}^{-1} & S_{32}^{-1} & S_{33}^{-1} \end{bmatrix}$$

$$S_{ij}^{-1} = \begin{bmatrix} b_0 & b_1 & \cdots & b_6 & b_7 \end{bmatrix}$$

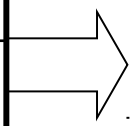
2-ое преобразование



$$\begin{bmatrix} b_0' \\ b_1' \\ b_2' \\ b_3' \\ b_4' \\ b_5' \\ b_6' \\ b_7' \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \times \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} = C_{ij}$$

3-ье преобразование

C_{00}	C_{01}	C_{02}	C_{03}
C_{10}	C_{11}	C_{12}	C_{13}
C_{20}	C_{21}	C_{22}	C_{23}
C_{30}	C_{31}	C_{32}	C_{33}



C_{00}	C_{01}	C_{02}	C_{03}
C_{11}	C_{12}	C_{13}	C_{10}
C_{22}	C_{23}	C_{20}	C_{21}
C_{33}	C_{30}	C_{31}	C_{32}

Матрица D

=

d_{00}	d_{01}	d_{02}	d_{03}
d_{10}	d_{11}	d_{12}	d_{13}
d_{20}	d_{21}	d_{22}	d_{23}
d_{30}	d_{31}	d_{32}	d_{33}

Следующее преобразование является перемешиванием столбцов матрицы D

На этом шаге каждый К-ый столбец матрицы D представляется в 16-ричной системе счисления как вектор над полем $GF(2^8)$ с образующим многочленом

$$p(x) = 1 + x + x^3 + x^4 + x^8$$

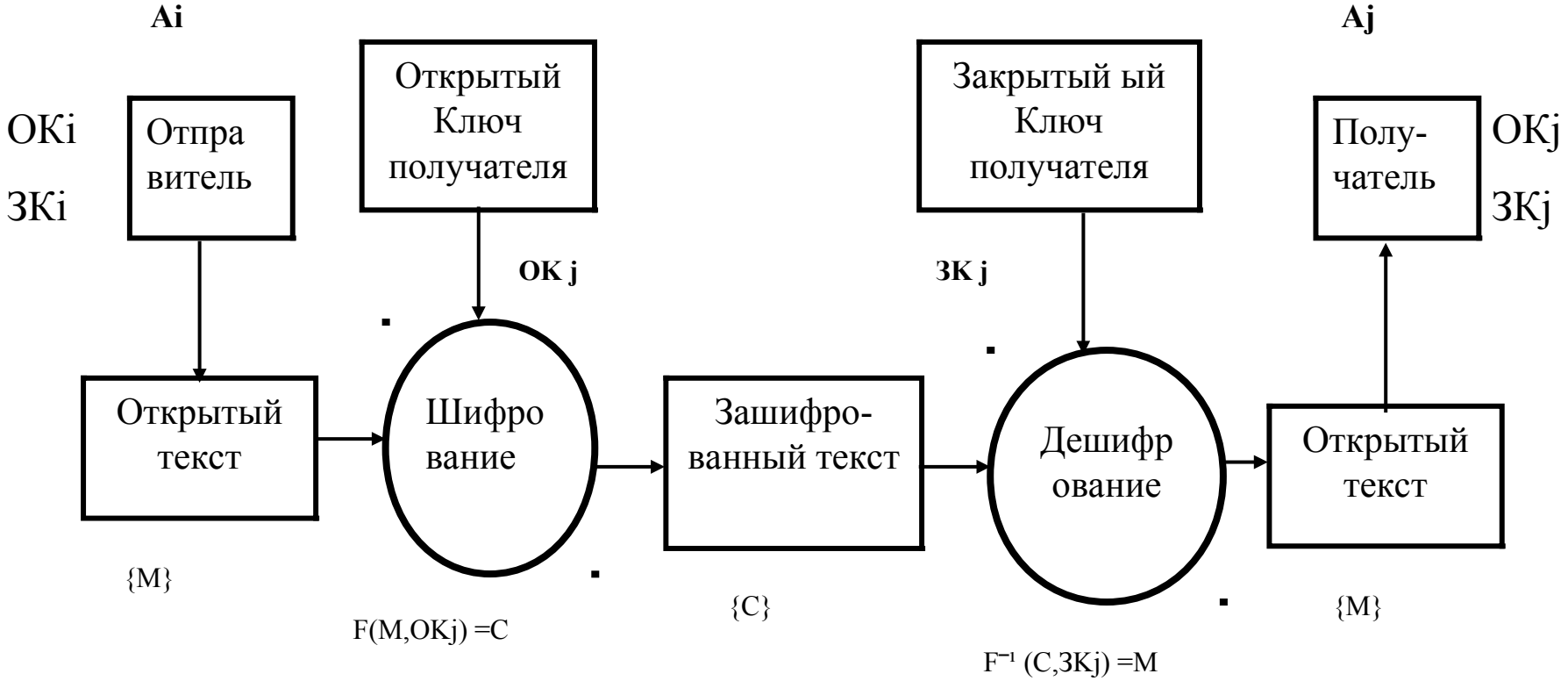
с дальнейшим умножением на определенную матрицу с элементами из этого же поля:

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \times \begin{bmatrix} D_{0K} \\ D_{1K} \\ D_{2K} \\ D_{3K} \end{bmatrix} = \begin{bmatrix} D'_{0K} \\ D'_{1K} \\ D'_{2K} \\ D'_{3K} \end{bmatrix}$$

Например, 02 = (0000 0010)

Наконец производится сложение всех 128 элементов полученной на предыдущем шаге матрицы D' с раундовым ключом. После завершения одного раунда все описанные выше операции повторяются с использованием других ключей. Количество раундов – 10, 12,14.

2) Ассиметричные ключи (использование пары ключей - открытого и закрытого)

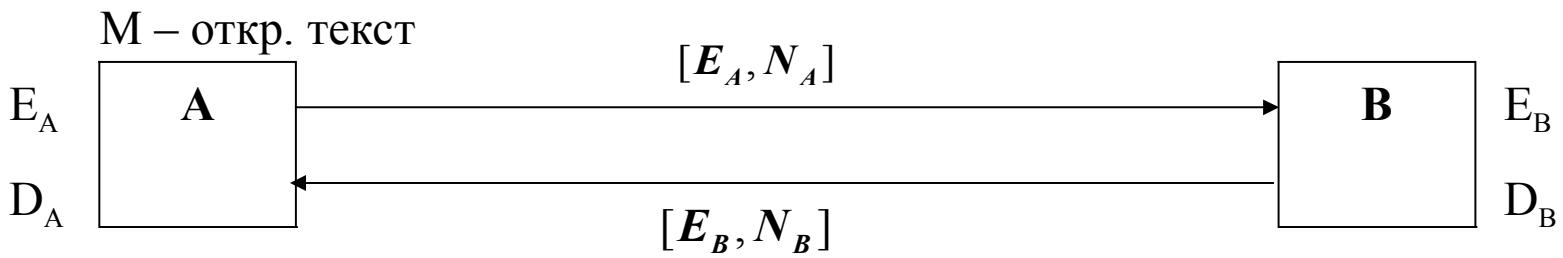


M – открытый текст, подлежащий шифрованию;
C – зашифрованный текст;
ОКj – открытый ключ шифрования получателя;
ЗКj – закрытый (секретный) ключ расшифрования получателя;
F(M,OKj) – функционал шифрования (криптографической защиты) сообщения оправ.;
F^{-1}(C,ЗKj) – обратный функционал расшифрования сообщения закрытым ключом получ.

Пример: стандарт RSA (Rivest, Shamir, Aldeman), США, Массачусетский Технологический институт, 1977 г.

RSA

1. Формирование ключа
   1. p и q – большие простые целые числа;
   2. $N=p\times q$
   3. $\varphi(N)=(p-1)\times(q-1)$ – функция Эйлера;
   4. Выбор открытого ключа $E<N$, такого, что $НОД(E, \varphi(N))=1$
   5. Определение закрытого ключа D:
      $E\cdot D\equiv 1 \bmod \varphi(N)$
      $НОД(D, \varphi(N))=1$



$p_A, q_A;$

$N_A = p_A \cdot q_A;$

$\varphi(N_A) = (p_A - 1)(q_A - 1);$

$E_A \cdot D_A \equiv 1 \bmod \varphi(N_A).$

$p_B, q_B;$

$N_B = p_B \cdot q_B;$

$\varphi(N_B) = (p_B - 1)(q_B - 1);$

$E_B \cdot D_B \equiv 1 \bmod \varphi(N_B).$

$$(M)^{E_B} = C \bmod N_B \Rightarrow C = \left[(M)^{E_B}\right]^{D_B} = (M)^{E_B \cdot D_B \equiv 1 \bmod \varphi(N_B)} = M \bmod N_B$$

Отправитель А

С – шифрованный текст

Получатель В

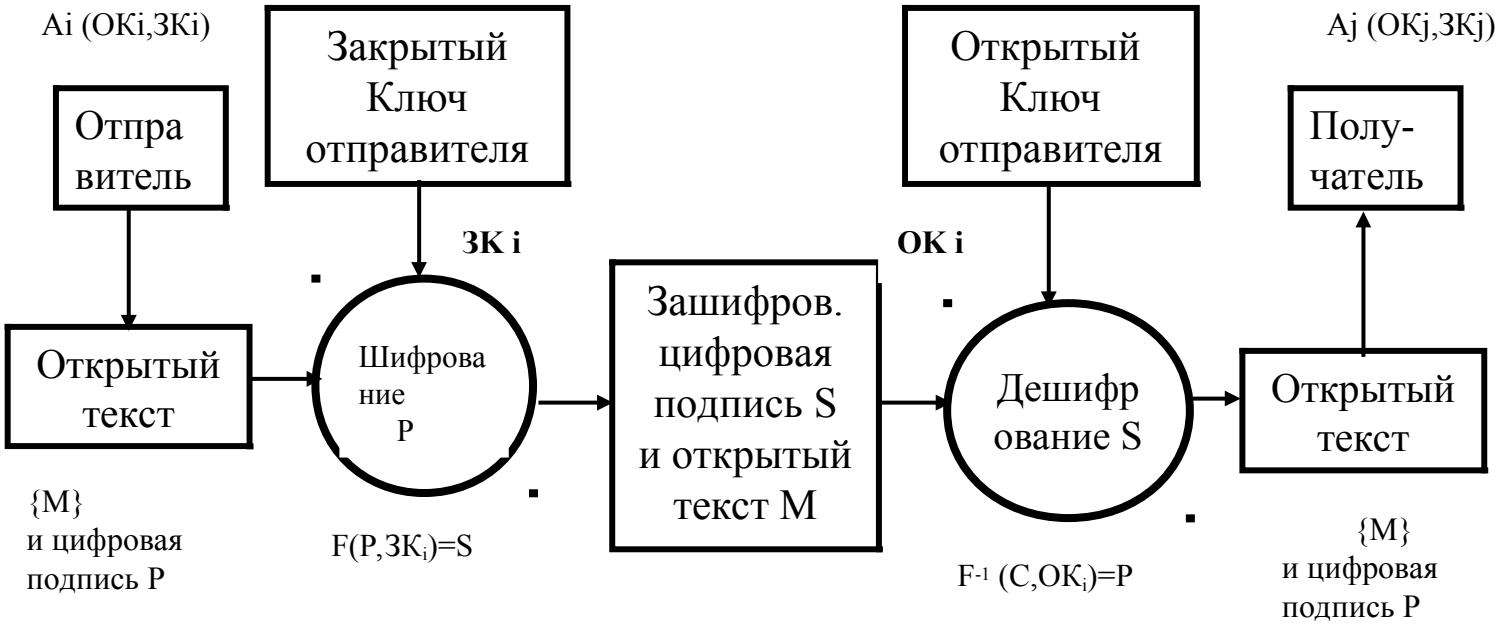
p и q – простые большие числа, например 100-разрядные. p и q - нечетные числа.

$\frac{10^{100} - 10^{99}}{2}$ - количество 100-разрядных нечетных чисел;

$\left[(10^{100} / \ln 10^{100}) - (10^{99} / \ln 10^{99})\right]$ - прибл. количество 100-разрядных простых чисел.

Вероятность успешного выбора одной пары 0,00868

3). Цифровая подпись (Аутентификация – подтверждение подлинности)

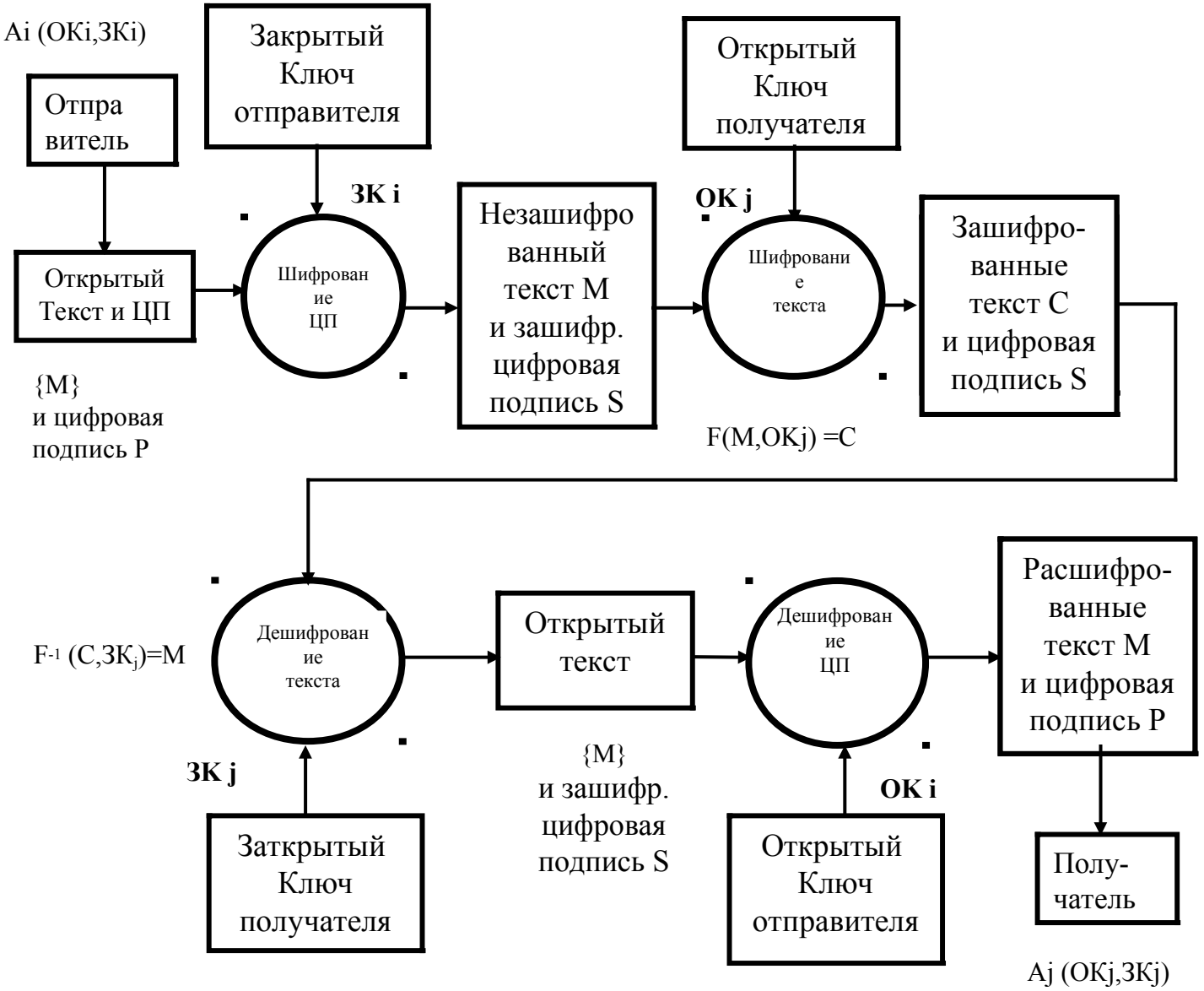


P –открытая цифровая подпись отправителя Ai;

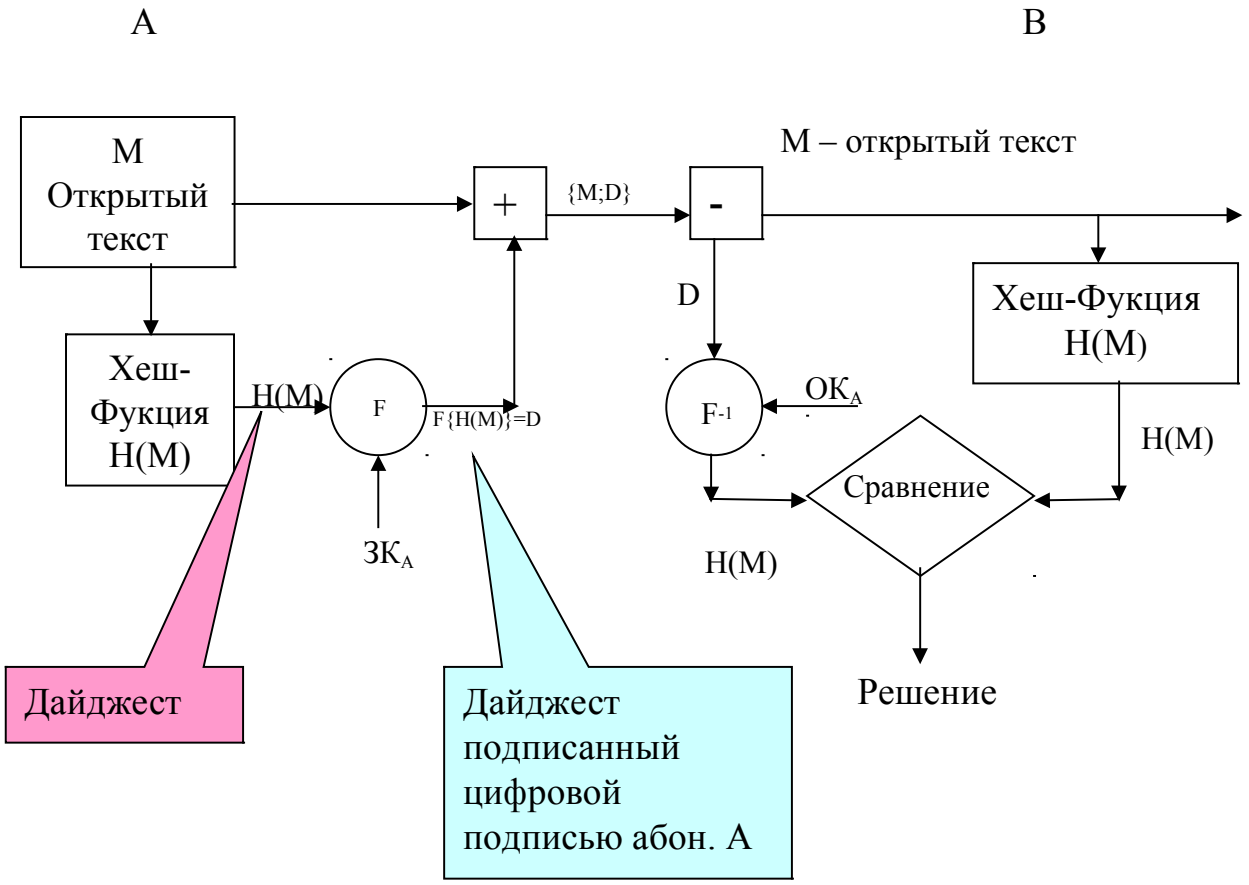
S – зашифрованная цифровая подпись отправителя Ai

Привести пример использования стандарта RSA для электронной цифровой подписи для p=7 и q=13 при условии, сообщение было подписано открытой цифровой пдписью «12» (Это может быть вычисленная хеш-функция).

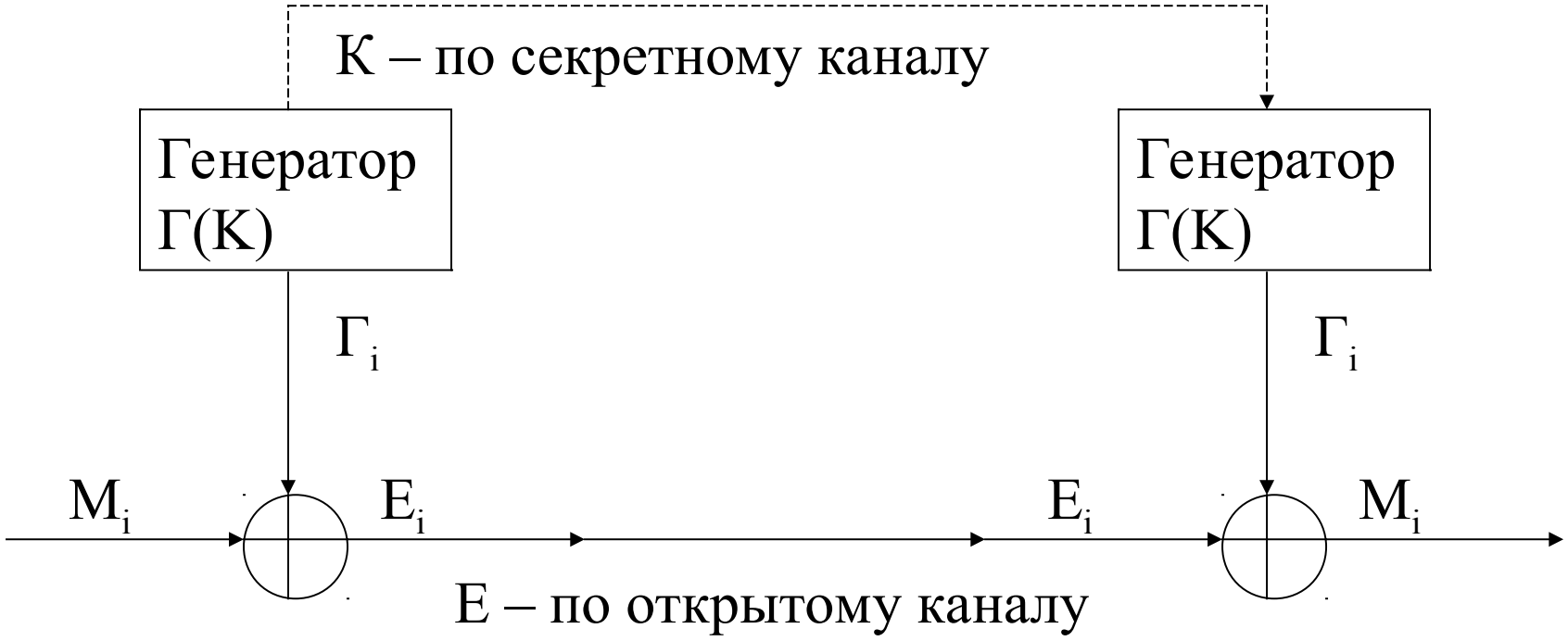
4). Раздельное шифрование текста и цифровая подпись. (Конфиденциальность и аутентификация)



5). Дайджест сообщения (проверка целостности сообщения) (хеш-функция – контрольная сумма, CRC и др.)



1.6. ПОТОКОВОЕ ШИФРОВАНИЕ (ШИФРОВАНИЕ ПСЕВДОСЛУЧАЙНЫМИ ПОСЛЕДОВАТЕЛЬНОСТЯМИ (СКРЕМБЛИРОВАНИЕ))



Г – шифрующая последовательность (М-последовательность)

Генераторы должны быть засинхронизированы

1.7. ПОБЛОЧНОЕ ШИФРОВАНИЕ ПСЕВДОСЛУЧАЙНЫМИ ЧИСЛАМИ

А	*Б*	*В*	*Г*	*Д*	*Е*	*Ж*	*З*	*И*	*Й*	*К*	*Л*	*М*	*Н*	*О*	*П*	*Р*
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
С	*Т*	*У*	*Ф*	*Х*	*Ц*	*Ч*	*Ш*	*Щ*	*Ъ*	*Ы*	*Ь*	*Э*	*Ю*	*Я*	*Пр*	
18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	

Алгоритм шифрования: $y_i \equiv x_i + b_i \mod 33$; Расшифрование: $y_i - b_i \equiv x_i \mod 33$;

x_i – номер буквы в открытом тексте,

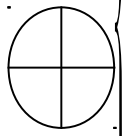
y_i – новый номер буквы алфавита в шифрованном тексте;

b_i – целое число от 0 до 33, соответствующее номеру i- ой буквы ключа и определяющее значение сдвига номера x

К	**Р**	**И**	**П**	**Т**	**О**	**Г**	**Р**	**А**	**Ф**	**И**	**Я**	← Открытый текст {x}
11	**17**	**09**	**16**	**19**	**15**	**04**	**17**	**01**	**21**	**09**	**32**	←x_i
b1	**b2**	**b3**	**b4**	**b5**	**b6**	**b7**	**b8**	**b9**	**b10**	**b11**	**b12**	←Ключевой секретный текст из случайных чисел b_i известных обоим абон.
04	**07**	**12**	**24**	**11**	**12**	**01**	**24**	**11**	**09**	**02**	**24**	
15	**24**	**21**	**07**	**30**	**27**	**05**	**08**	**12**	**30**	**11**	**23**	←y_i
Я	**Ч**	**Ф**	**Ж**	**Э**	**Ъ**	**Д**	**З**	**Л**	**Э**	**К**	**Ц**	←Зашифрованный текст {y}

Криптоустойчивость существенно повышается, так как числа b_i для каждой буквы будут различными, формируемыми датчиком случайных чисел.

Поблочное шифрование (сложение может осуществляться по **mod2)**



П (16)	**Р (17)**	**И (09)**	**К (11)**	**А (01)**	**З (08)**	←Открытый текст
10000	**10001**	**01001**	**01011**	**00001**	**01000**	
02	**01**	**17**	**09**	**14**	**15**	←Случайные числа (секретный ключ)
00010	**00001**	**10001**	**01001**	**01110**	**01111**	
10010	**10000**	**11000**	**00010**	**01111**	**00111**	
18	**16**	**24**	**02**	**15**	**07**	
С	**П**	**Ч**	**Б**	**О**	**Ж**	←Шифрованный текст

1.7. ПОЛИГРАММНЫЙ ШИФР ЗАМЕНЫ ХИЛЛА

А	*Б*	*В*	*Г*	*Д*	*Е*	*Ж*	*З*	*И*	*Й*	*К*	*Л*	*М*	*Н*	*О*	*П*	*Р*
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
С	*Т*	*У*	*Ф*	*Х*	*Ц*	*Ч*	*Ш*	*Щ*	*Ъ*	*Ы*	*Ь*	*Э*	*Ю*	*Я*		
18	19	20	21	22	23	24	25	26	27	28	29	30	31	32		

$N=32$ – число букв в алфавите

m - *грамма случайных чисел* $f=\{f_1, f_2, ..., f_m\}$;

m - *грамма открытого текста* $\rightarrow x=(x_1, x_2, ..., x_m)$

m - *грамма шифрованного текста* $\rightarrow y=(y_1, y_2, ..., y_m)$

A - *матрица* $(m \times m)$

Переменные **f**, **x** и **y** являются десятичными цифрами, соответствующими буквам русского алфавита.

Переменные x_i и y_i состоят из m цифр каждая.

ПРИМЕР РАБОТЫ ПОЛИГРАММНОГО ШИФРА ХИЛЛА

N=32, m = 2, Открытый текст: «КРИПТОГРАФИЯ»

А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я		
18	19	20	21	22	23	24	25	26	27	28	29	30	31	32		

$$A=\begin{bmatrix}5 & 8\\ 3 & 5\end{bmatrix};\quad A^{-1}=\begin{bmatrix}5 & 24\\ 29 & 5\end{bmatrix};\quad f=\begin{bmatrix}f_1 & f_2\end{bmatrix}=\begin{bmatrix}4 & 2\end{bmatrix};$$

Правило шифрования: $\mathbf{y = xA + f}$ modN;

Правило расшифрования: $\mathbf{x = (y - f)A^{-1}\ modN}$

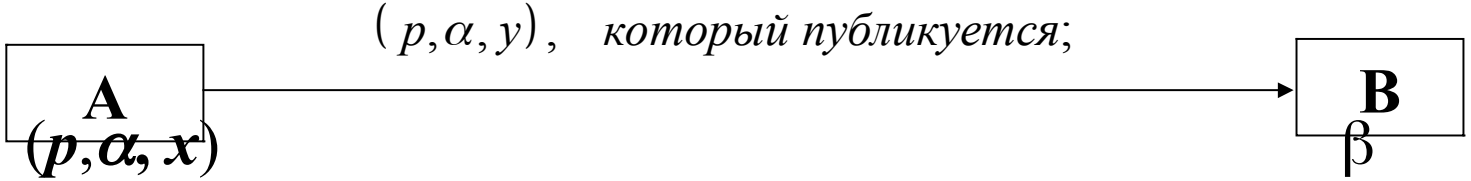
К,Р	И,П	Т,О	Г,Р	А,Ф	И,Я	←Открытый текст
11,17	9,16	19,15	4,17	1,21	9,0	←{X} Цифры открытого текст
14,15	…	…	…	…	17,10	←{Y}Цифры после шифрования
Н,О	…	…	…	…	Р,Й	←Зашифрованный текст

Повторение отдельных вопросов Лекции 2:

1) Стандарт RSA (Пример: p=3, q=11);
2) Полиграммный шифр замены Хилла.
3) Вопросы и задачки к экзамену.

Лекция 3. Алгоритм шифрования методом Эль-Гамаля. Алгоритм дистанционного формирования общего сеансового ключа по методу Диффи-Хеллмана. Протокол Шамира дистанционного определения общего секретного ключа

Шифрование с открытым ключом по алгоритму Эль-Гамаля.



Что делает абонент А?

1) **Выбирает большое простое целое число *p* с помощью датчика простых чисел;**
2) **Выбирает примитивный элемент α** $(2 \le \alpha \le p-2)$;
3) **Выбирает случайное число *x – секрет абонента А, 1*** $\le x \le p-1$, т.е. его закрытый ключ $ЗК_A = x = D_A$;
4) **Вычисляет** $y = \alpha^x \pmod p$;
5) **Создает свой открытый ключ** $ОК_A = E_A = (p,\alpha,y)$, *который публикуется*;

Шифрование абонентом **B** на открытом ключе абонента **A** по алгоритму Эль-Гамаля

Абонент B:

1) Извлекает открытый ключ абонента **A:**

$$ОК_A = (p, \alpha, y) = (p, \alpha, y = \alpha^x),\ где\ x - секрет\ A.$$

2) Формирует сообщение MЄ[1,p–1];

3) Выбирает случайное число β, [1,p–1];

4) Вычисляет два числа: $a = \alpha^{\beta} \pmod p$; $b = M \cdot y^{\beta} \pmod p$;

5) Создает шифрованное сообщение C: C=(a,b) и отправляет A

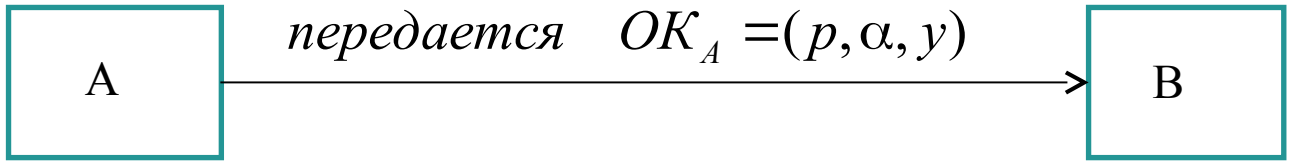
Расшифровка на стороне A:

1) Используя $ЗК_A = x$, вычисляет

$$\frac{b}{a^x} = \frac{M \cdot y^{\beta}}{(\alpha^{\beta})^x} = \frac{M(\alpha^x)^{\beta}}{\alpha^{\beta x}} = M \pmod p.$$

Рассмотреть пример: p=13, x=7, β=8, M=4.

Электронная цифровая подпись по алгоритму Эль-Гамаля



$ЗК_A = x$ - *простое число*, $\in [1, p-1]$;

$ОК_A = (p, \alpha, y)$, *где* $y = \alpha^x \pmod p$;

$\beta \in [1, p-1]$ – взаимно простое с (p-1)

Абонент А: Сообщение - “m”;

Вычисляется хеш от передаваемого сообщения h=H(m) mod(p-1)

Находит два числа a и b: $a = \alpha^{\beta} \pmod p$; $b = \dfrac{h - x \cdot a}{\beta} \bmod (p-1)$;

Сообщение подписывается зашифрованной подписью $S(m)=(a,b)$

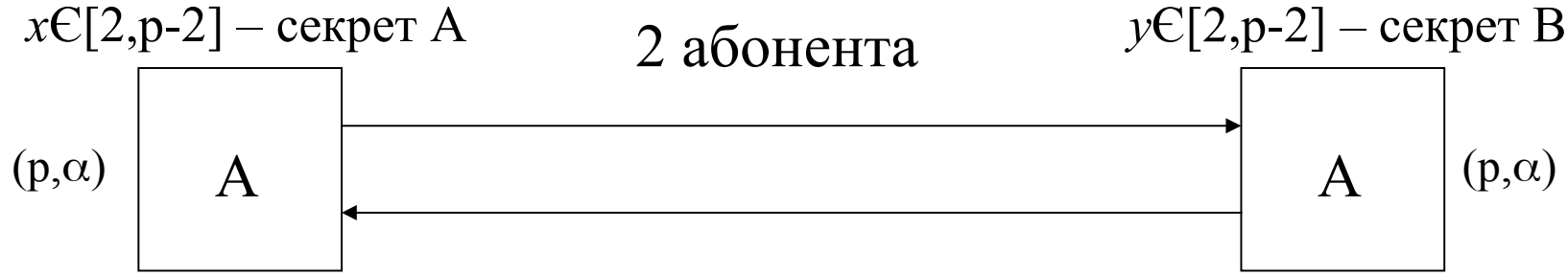
И передается абоненту В сообщение с шифрованной подписью $(m, S(m))$.

Абонент В вычисляет по принятому сообщению хеш: h=H(m) mod(p-1)

На стороне В:

$f_1 = \alpha^h \pmod p$; $f_2 = y^a \cdot a^b = (\alpha^x)^a \cdot a^b = (\alpha^x)^a \cdot (\alpha^{\beta})^{\frac{h - xa}{\beta}} = \alpha^h \pmod p$; *т.е.* $f_1 = f_2$.

Системы с общим секретным ключом по протоколу Диффи-Хеллмана (1976)



p – большое простое число;

α – примитивный элемент.

$$\alpha^{p-1} \equiv 1 \bmod p$$

1) Обмен: $A \to B$: $\alpha^x \pmod p$; $B \to A$: $\alpha^y \pmod p$;

2) А формирует ключ: $K_A = (\alpha^y)^x \bmod p$;

3) В формирует ключ: $K_B = (\alpha^x)^y \bmod p$;

Получается одинаковый, т. е. **общий секретный ключ**: $К_А = К_В = К$

Рассмотреть пример: $p=7$; $x=2$; $y=5$.

3 абонента (протокол Диффи-Хеллмана)

x y z

A, B, C

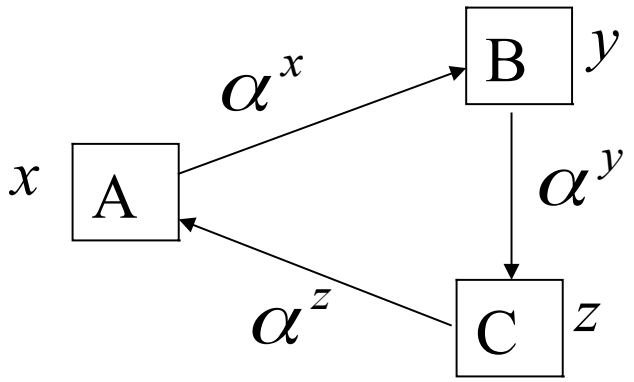
(p,α)

1-ый раунд:

$A \to B: \quad \alpha^x \bmod p;$

$B \to C: \quad \alpha^y \bmod p;$

$C \to A: \quad \alpha^z \bmod p.$

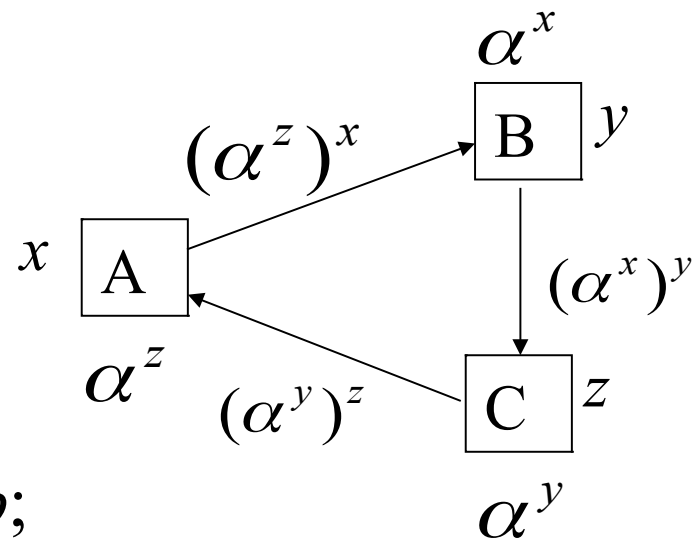


2-ой раунд:

$A \to B: \quad (\alpha^z)^x \bmod p;$

$B \to C: \quad (\alpha^x)^y \bmod p;$

$C \to A: \quad (\alpha^y)^z \bmod p.$



3-ий раунд:

$A \to B: \quad K_A = (\alpha^{yz})^x = \alpha^{xyz} \bmod p;$

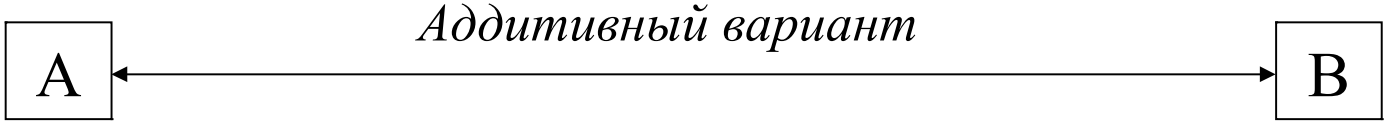
$B \to C: \quad K_B = (\alpha^{zx})^y = \alpha^{xyz} \bmod p;$

$C \to A: \quad K_C = (\alpha^{xy})^z = \alpha^{xyz} \bmod p.$

Общий сеансовый ключ: $К_А=К_В=К_С=К$

Получение общего сеансового секретного ключа К по протоколу Шамира

Аддитивный вариант

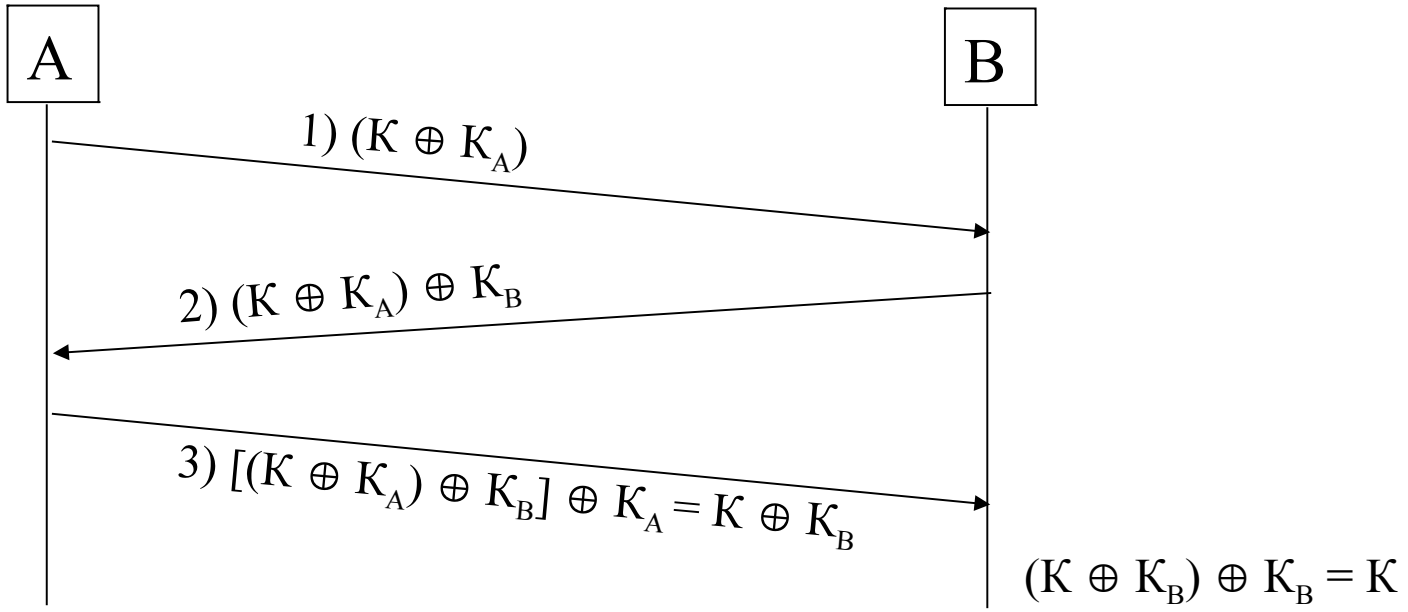


Абонент А имеет:

1) Секретную ПСП К;
2) Дополнит.секретн.ПСП $К_А$.

Абонент В имеет:

1) Секретную ПСП $К_В$.

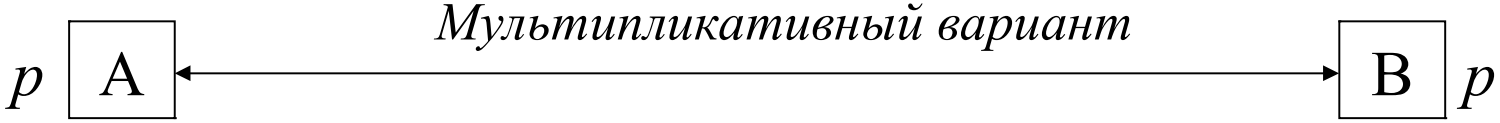


Недостаток: 1) ⊕ 2) ⊕ 3) =К (перехват и сложение ⊕)

Абонент В узнаёт секретный ключ К

Получение общего сеансового секретного ключа К по протоколу Шамира

Мультипликативный вариант



Оба абонента знают большое простое число p.

Абонент А:

1) задает секретный ключ К;
2) выбирает число a взаимно простое с (p-1);
3) находит число c, взаимно простое с a, т. е. такое, что

$$a \cdot c \equiv 1 \bmod(p-1)$$

Абонент В:

1) выбирает число b взаимно простое с (p-1);
2) находит число d, взаимно простое с b, т. е. такое, что

$$b \cdot d \equiv 1 \bmod(p-1)$$