# 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.

**Лекция 1.**

**Законодательные и нормативные документы по защите информации.**

9 сентября 2000 г. Президентом Российской Федерации В. Путиным утверждена *Доктрина Информационной Безопасности Российской Федерации*, в которой определены, в частности, следующие задачи:

- разработка, использование и совершенствование средств защиты информации и методов контроля эффективности этих средств, развитие защищенных телекоммуникационных систем, повышение надежности специального программного обеспечения;
- создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации и специальных воздействий, вызывающих разрушение, уничтожение, искажение информации, а также изменение штатных режимов функционирования систем и средств информатизации и связи;
- сертификация средств защиты информации, лицензирование деятельности в области защиты государственной тайны, стандартизация способов и средств защиты информации;

*Безопасность компьютерных технологий и электронных информационных сетей в настоящее время, в век всеобъемлющей цифровизации, выходит на первый план и становится объектом национальной безопасности, безопасности государства.*

.

- **Федеральный закон РФ от 27.07.2006 г. №149-ФЗ “Об информации, информатизации и защите информации”** Даны определения терминов и приведены основные положения в области телекоммуникационных систем и информационной безопасности.

**ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ.**

**Защита информации –** это защита (сохранение целостности и конфиденциальности) информации от несанкционированного доступа.

**Целостность информации** – это сохранение ее в первоначальном виде.

**Конфиденциальность** – означает, что информация должна быть получена только тем, кому она и предназначалась.

# ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ (продолжение).

| | |
|---|---|
| 1. Доступ к информаии | *Ознакомление с информацией, ее обработка, копиро-вание, модификация или уничтожение* |
| 2. Правила разграничения доступа | *Правила, регламентирующие права доступа* |
| 3.Санкционированный доступ | *Доступ к информации, не нарушающий правила розграничения доступа* |
| 4.Несанкционированный доступ | *Доступ к информации, нарушающий правила розграничения доступа* |
| 5.Несанкционированные действия | *Несанкционированные действия нарушителя, выражающиеся в разрушении, хищении, модификации информации или ознакомлении с ее содержанием* |

| | |
|---|---|
| 6. Защита от НСД | *Предотвращение или существенное затруднение НСД* |
| 7. Срдства защиты от НСД | *Программные, технические или программно-технич. средства, предназначенные для защиты от НСД* |
| 8. Субъект доступа | *Лицо или процесс, действия которых регламентируются правилами разграничения доступа* |
| 9. Объект доступа | *Информационный ресурс, доступ к которому регламентируется правилами разграничения доступа* |
| 10.Идентификатор доступа | *Уникальный признак субъекта или объекта доступа* |
| 11.Пароль | *Идентификатор субъекта доступа, который является его (субъета) секретом* |
| 12.Аутентификация | *Проверка принадлежности субъекту доступа предъявленного им идентификатора (подтверждение подлинности)* |

**Шифрование — обратимое преобразование информации в целях сокрытия от сторонних** (неавторизованных) лиц, с предоставлением, в это же время, авторизованным легитимным пользователям доступа к ней. Главным образом, шифрование служит задачей соблюдения конфиденциальности передаваемой информации.
**Криптография — наука о методах обеспечения конфиденциальности и аутентичности** (целостности и подлинности авторства, а также невозможности отказа от авторства) информации.

*Традиционная криптография включает в себя симметричные криптосистемы, в которых шифрование и расшифрование проводится с* использованием одного и того же секретного ключа (ключей). *Помимо этого, современная* криптография включает в себя *асимметричные криптосистемы, системы электронной цифровой подписи (ЭЦП), хеш-функции, управление распространением ключей и другие новые методы криптографии, например квантовую криптографию.*
***Стеганография — это наука о скрытой передаче информации путём сохранения в тайне*** самого факта передачи. Стеганографию обычно используют совместно с методами криптографии, дополняя её.

**Криптоаналитик –** это нелегальный пользователь (злоумышленник) , который стремится получить несанкционированный доступ к информации и ее дешифрования.

**Криптоустойчивость** криптосистемы определяется числом стандартных операций, которые нелегальный пользователь должен выполнить для достижения цели, не зная при этом ключей шифрования.

**Двоичная (битовая) криптоустойчивость** (сложность) определяется количеством двоичных операций для достижения цели.

**Криптоатака** – попытка нелегального пользователя (криптоаналитика) получить информацию.

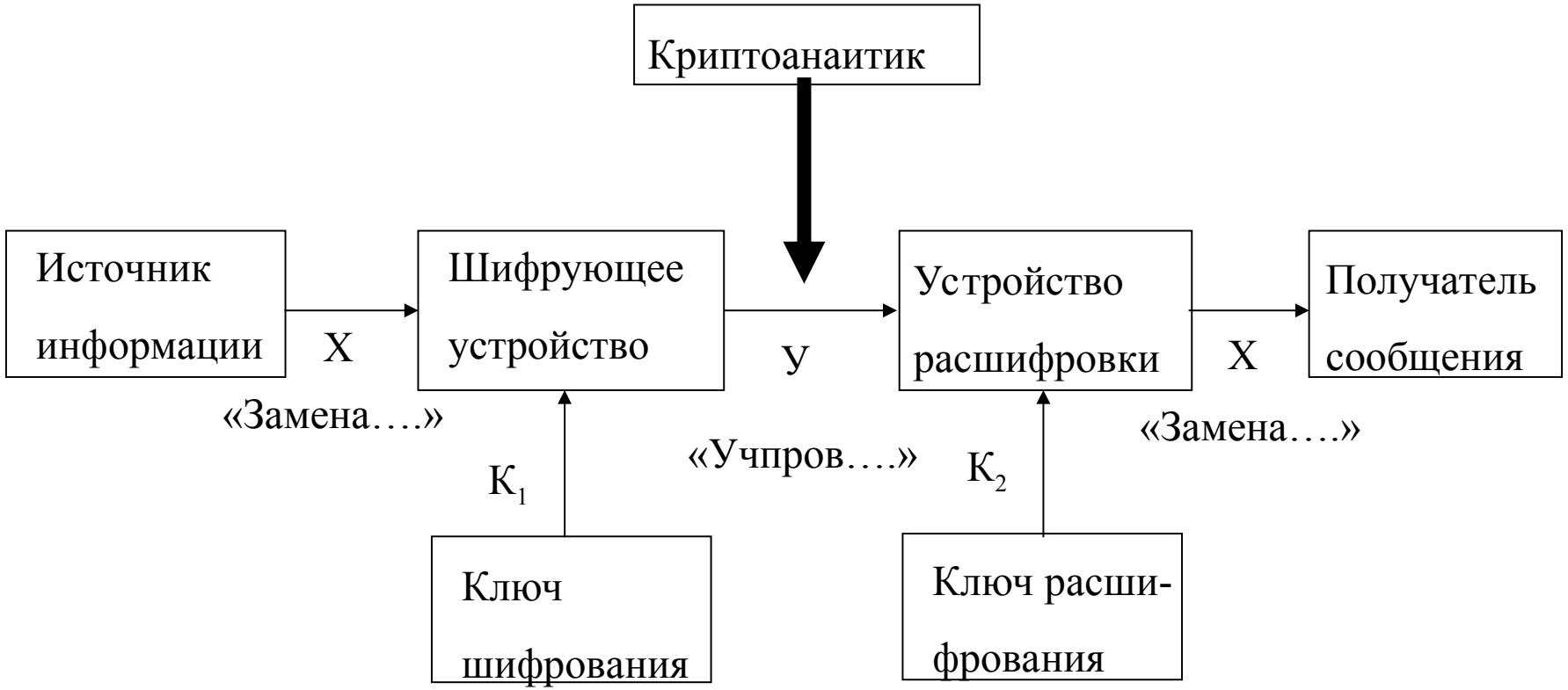
**Пассивный криптоаналитик** может осуществлять подслушивание и (или) перехват зашифрованного сообщения, не нарушая при этом процесс обмена зашифрованными сообщениями между отправителем и получателем.

**Активный криптоаналитик** может подслушивать, перехватывать и преобразовывать сообщения по своему усмотрению: задерживать, искажать, имитировать создание новых сообщений, устраивать обрыв связи и т.п. В этом случае одновременно нарушается  и целостность передаваемого сообщения, и конфиденциальность.

**Взлом или вскрытие криптосистемы** – удачная попытка получения информации нелегальным пользователем. Метод вскрытия криптосистемы называется **криптоанализом.**

**Временная криптоустойчивость** – это время (от нескольких месяцев до года и более), которое может затратить нелегальный пользователь для взлома криптосистемы.

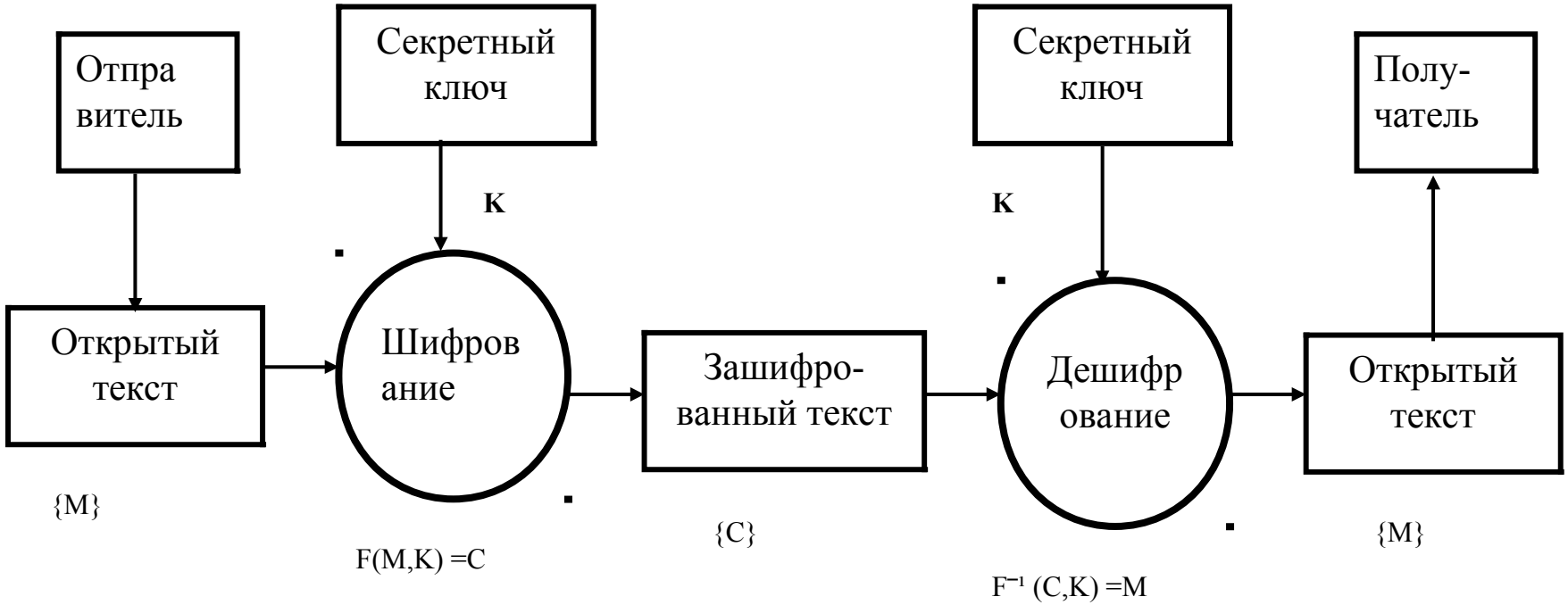
# ОБЩАЯ БДОК-СХЕМА СИСТЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ С КРИПТОЗАЩИТОЙ




X – открытый текст

У – зашифрованный текст

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




M – открытый текст, подлежащий шифрованию;

C – зашифрованный текст;

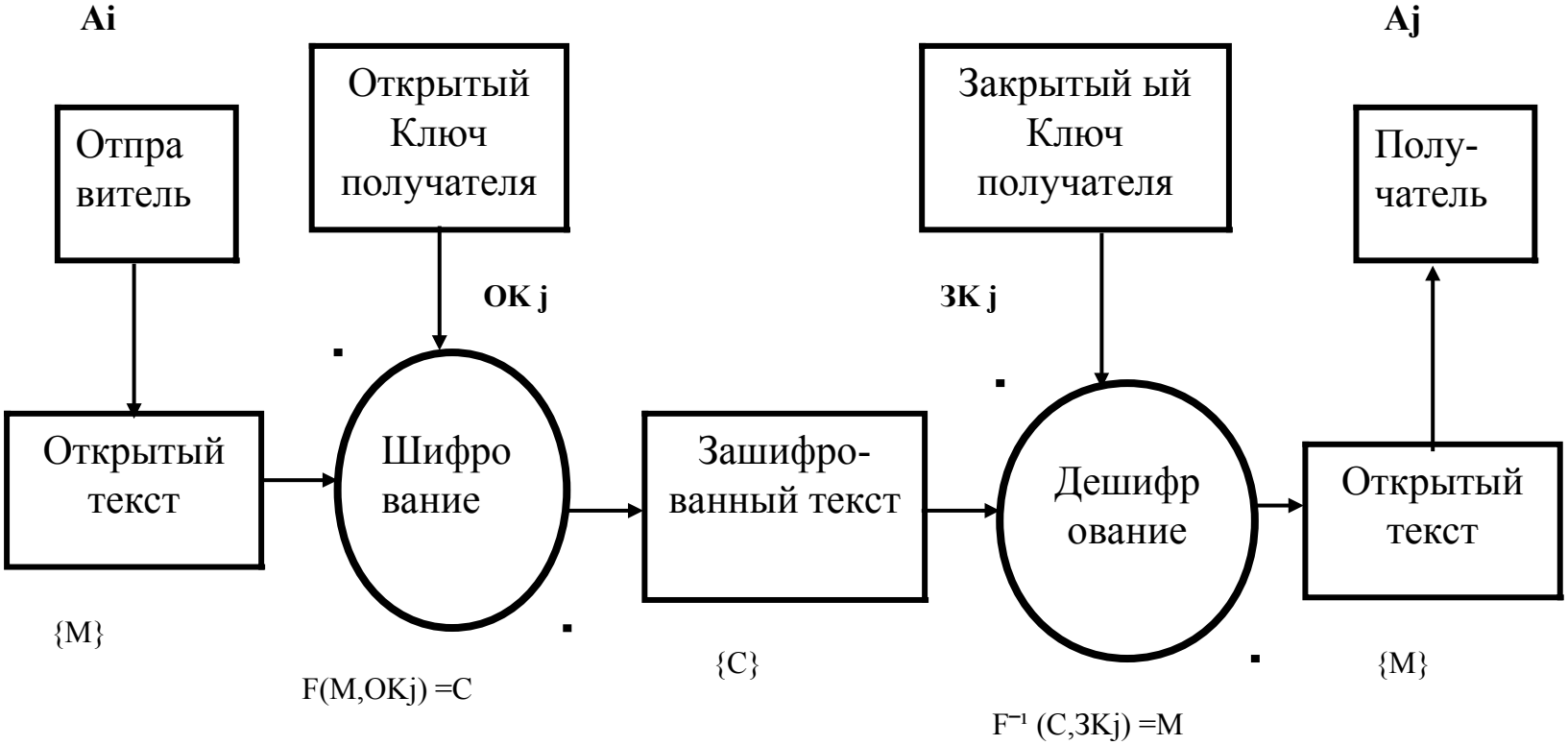
K – общий секретный ключ шифрования;

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.**

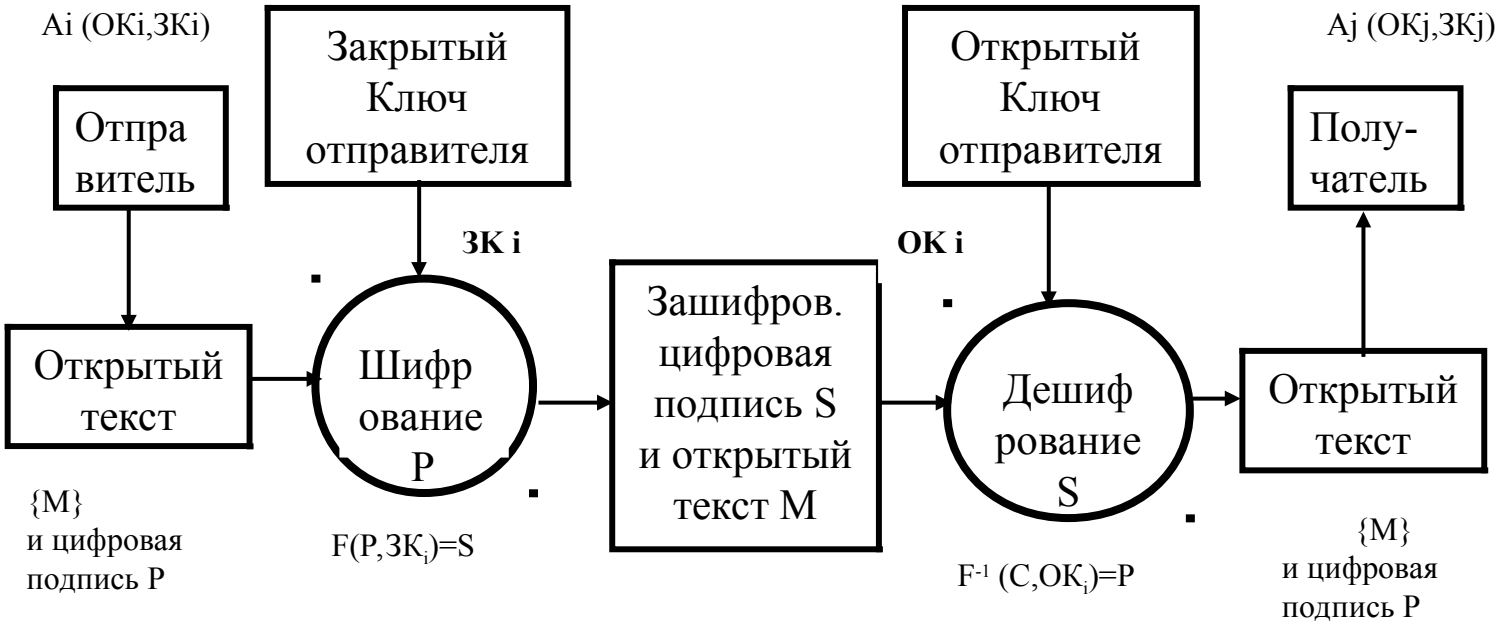
## 2) Ассиметричные ключи (использование пары ключей - открытого и закрытого)




M – открытый текст, подлежащий шифрованию;
C – зашифрованный текст;
OKj – открытый ключ шифрования получателя;
ЗKj – 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.**

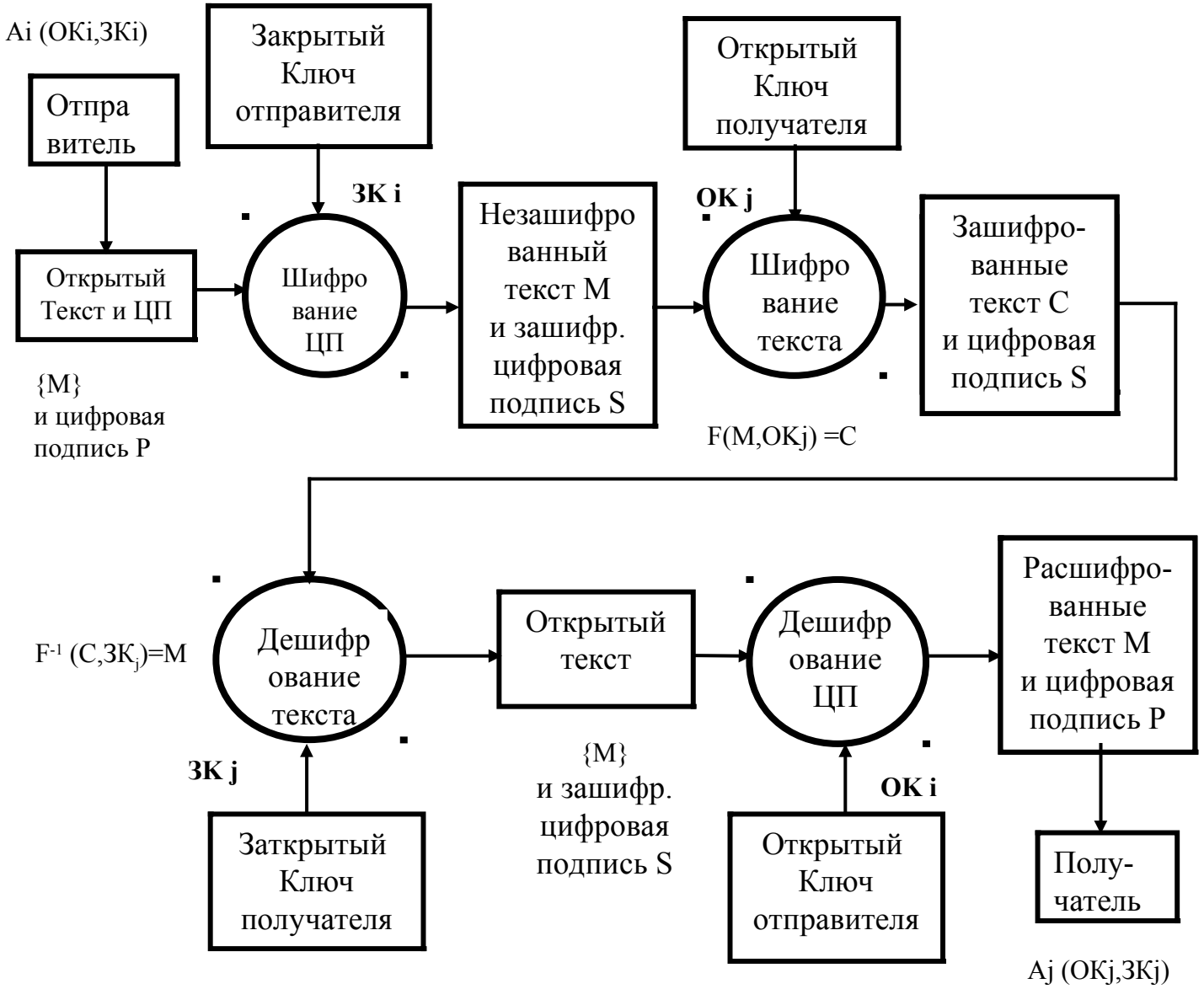
## 3). Цифровая подпись (Аутентификация – подтверждение подлинности)



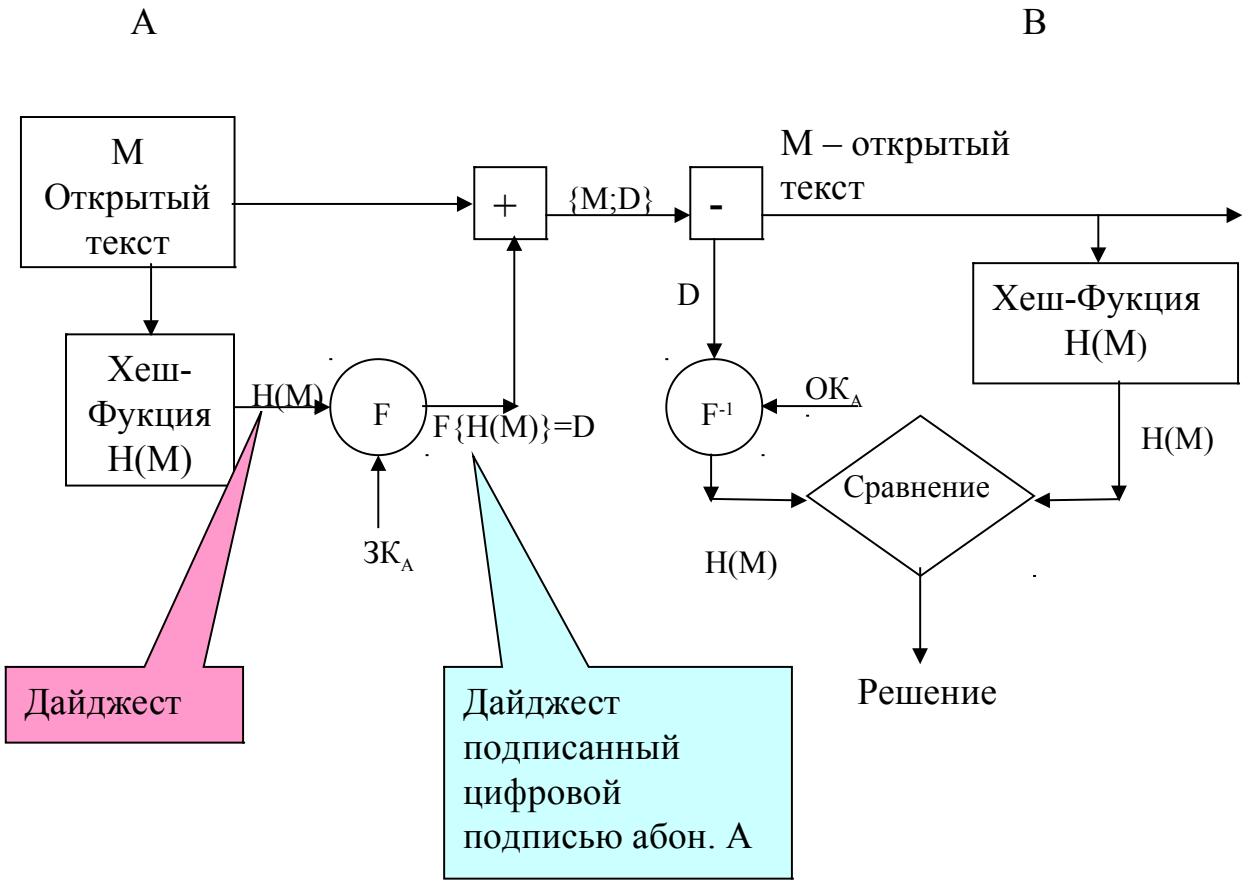

P –открытая цифровая подпись отправителя Ai;

S – зашифрованная цифровая подпись отправителя Ai

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



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



# 1. МЕТОДЫ ЗАМЕНЫ (ПОДСТАНОВКИ)

## 1.1. Моноалфавитная замена

1.1. Шифр Цезаря.

| A | B | C | D | E | ….. | X | Y | Z |
|---|---|---|---|---|---|---|---|---|
| ↓↑ | ↓↑ | ↓↑ | ↓↑ | ↓↑ | | ↓↑ | ↓↑ | ↓↑ |
| C | D | E | F | G | …… | Z | A | B |

Исходный алфавит

Смещенный алфавит на К=2 влево

К – размер ключа шифрования (секрет);

↓- шифрование путем замены буквы верхнего ряда буквой шифроключа (нижнего ряда);

↑ - расшифровывание путем обратной замены буквы шифрованного текста из нижнего ряда буквой алфавита из верхнего ряда.

Аналогично в русском алфавите.

Открытый текст Зашифрованный текст

ИЗУЧАЙТЕКРИПТОГРАФИЮ → ЛКЦЪГМХИВНУЛТСЖУГЧЛА

**Недостаток** – для дешифрования криптоаналитик может использовать известное распределение вероятностей отдельных букв и корреляционные связи между ними.

## 1.2. Аддитивный шифр замены (Аналог Шифра Цезаря )

| 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 | 9 | 16 | 19 | 15 | 4 | 17 | 1 | 21 | 9 | 32 | |
| К | Л | Ю | Ч | К | Л | Ю | Ч | К | Л | Ю | Ч | ←Ключевой секретный текст |
| 11 | 12 | 31 | 24 | 11 | 12 | 31 | 24 | 11 | 12 | 31 | 24 | |
| 22 | 29 | 7 | 7 | 30 | 27 | 2 | 8 | 12 | 33 | 7 | 23 | |
| Х | Ь | Ж | Ж | Э | Ъ | Т | З | Л | Пр | Ю | Ц | ←Зашифрованный текст {y} |

**Криптоустойчивость** существенно повышается, так как число $b_i$ для каждой буквы будет различным.

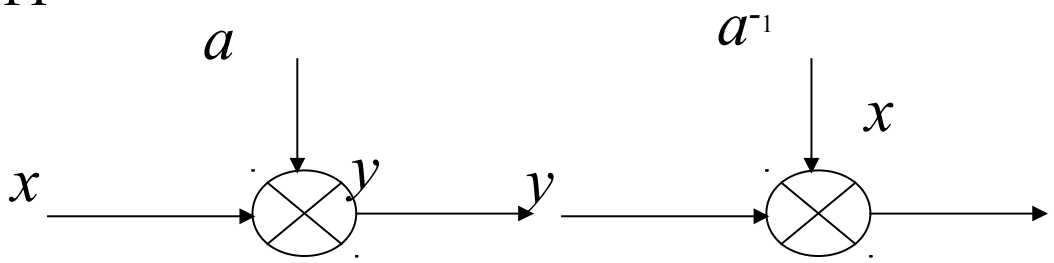
## 1.3.МУЛЬТИПЛИКАТИВНЫЙ ШИФР ЗАМЕНЫ

$y = ax \bmod n$ - правило шифрования

$x \in \{0,1,2,.....,N\}, N \le n-1;$

$x = ya^{-1}$ - дешифрование

$a$ - целое постоянное число



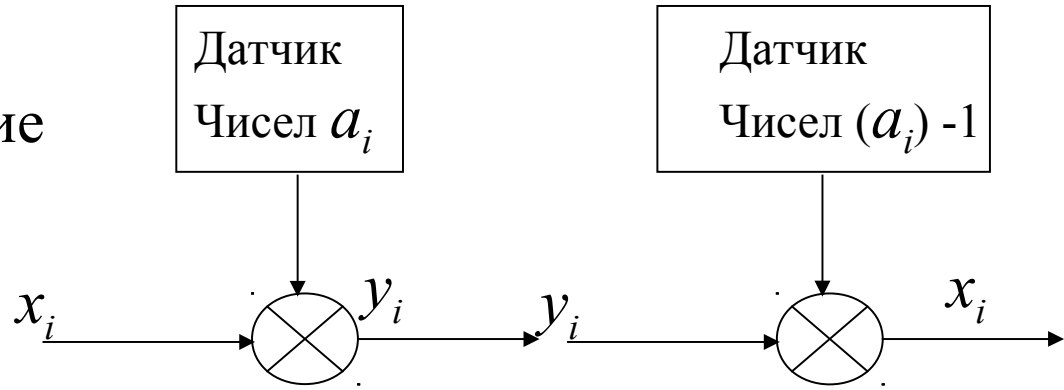

---

$y_i = a_i x_i \bmod n$ - правило шифрования

$x_i \in \{0,1,2,.....,N\}, N \le n-1;$

$x_i = y_i (a_i)^{-1}$ - дешифрование

$a_i$ - целые различные числа




---

### 1.4. АФФИННЫЙ ШИФР

$y = ax + b \bmod n$ - шифрование; Ключ $K(a,b)$

$x = (y - b)a^{-1} \bmod n$ - дешифрование $НОД(a,b) = 1.$

## 1.5. ПОЛИАЛФАВИТНЫЕ ШИФРЫ

Первые полиалфавитные шифры в европейских странах появились в эпоху Возрождения.Итальянский архитектор Баттиста Альберти (1404 – 1472) изобрел полиалфавитный шифр, который впоследствии получил имя дипломата XVI века Блеза де Виженера. В самом простом виде шифр Виженера строится в виде таблицы (квадрата) из циклически сдвинутых копий латинского алфавита, в которой буквы J и V исключены.

**Первая строка и первый столбец** – буквы алфавита в обычном порядке. Строки таблицы – циклически сдвинутые строки первой строки алфавита.

Для шифрования открытый текст располагается над первой строкой матрицы, а ключевая последовательность в виде столбца располагалась слева от матрицы.

Алгоритм шифрования: буква открытого текста $x_i$ заменяются на букву, которая стоит на пересечении столбца, соответствующего букве $x_i$ , и строки матрицы, соответствующей букве ключевого текста.

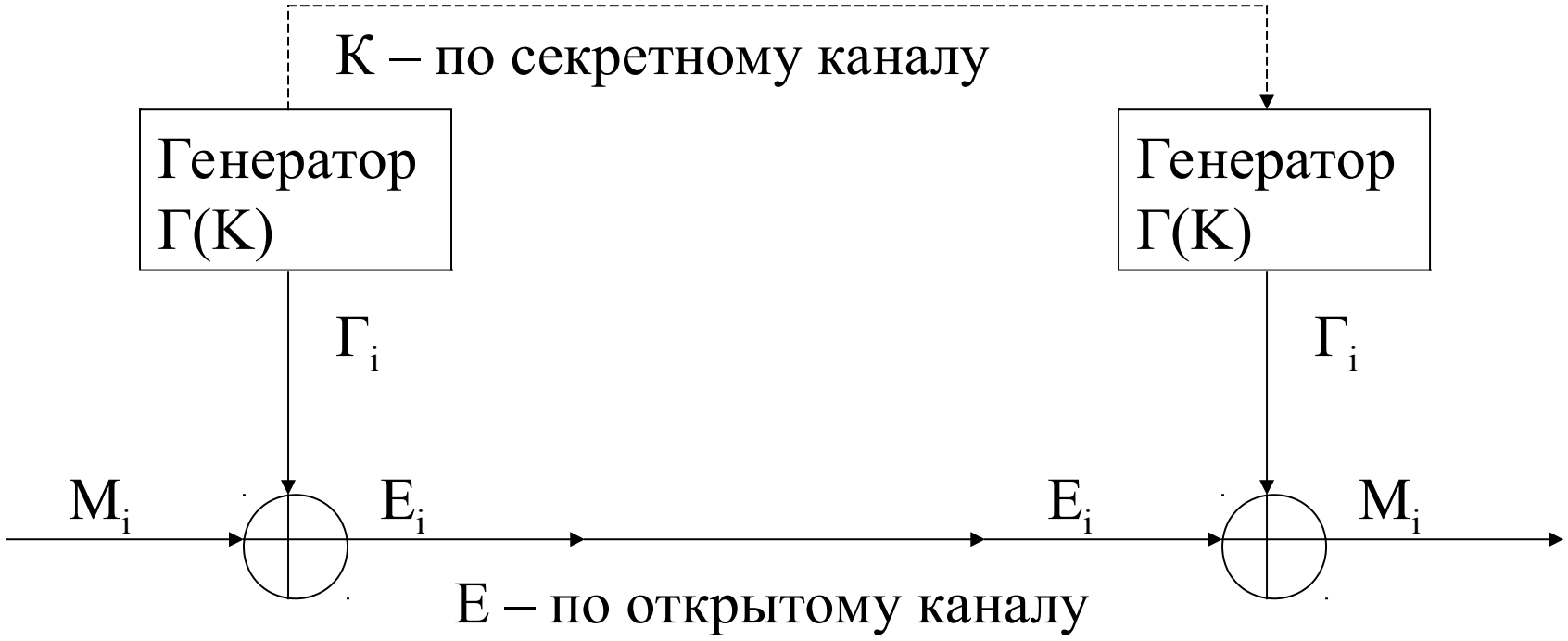
# Шифрование по таблице ВИЖЕНЕРА



| ↓/→ | 9 | | | 7 | | | | | 3 11 | 1 | | | | 6 | 4 | 2 8 | | 5 | | 10 | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | А | Б | В | Г | Д | Е | Ж | З | И | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ь | … |
| В | Г | Д | Е | Ж | З | И | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ь | Ъ | Ы | Э | |
| Е | Ж | З | И | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ь | Ъ | Ы | Э | Ю | Я | | А |
| Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ь | Ъ | Ы | Э | Ю | Я | | А | Б | В | Д | Е | Ж | З | И |
| Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ь | Ъ | Ы | Э | Ю | Я | | А | Б | В | Д | Е | Ж | З | И | К | Л | М | Н | О |
| И | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ь | Ъ | Ы | Э | Ю | Я | | А | Б | В | Г |
| Л | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ь | Ъ | Ы | Э | Ю | Я | | А | Б | В | Г | Д |
| Ь | Ь | Ъ | Ы | Э | Ю | Я | | А | Б | В | Д | Е | Ж | З | И | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | |

| К | Р | И | П | Т | О | Г | Р | А | Ф | И | Я | ←Открытый текст |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | |
| Н | Ц | Ц | А | Ъ | Ш | Э | У | Г | А | Ъ | Ж | ←Шифрованныйтекст |
| В | Е | Н | Т | И | Л | Ь | В | Е | Н | Т | И | ←Ключевое слово - ВЕНТИЛЬ |

# 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,

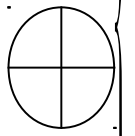
$y_i$ – новый номер буквы алфавита в шифрованном тексте;

$b_i$ – 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 |

К следующей лекции повторить из курса «Математические основы теории помехоустойчивого кодирования» следующие понятия:



- *простое целое число;*
- *взаимно простые числа;*
- *приведение целых чисел по* mod*p;*
- *определение группы, аддитивная и мультипликативная единица группы;*
- *порядок группы;*
- *циклическая группа;*
- *порядок элемента группы;*
- *первообразный элемент группы;*
- *сущность малой теоремы Ферма;*
- *функция Эйлера от целого числа;*
- *функция Эйлера от простого целого числа;*
- *сущность теоремы Эйлера;*
- *поле простое и поле расширенное;*
- *примитивный элемент поля и примитивный многочлен, образующий расширенное поле.*

Задание на дом по материалу 1-ой лекции:

• Заполнить полностью таблицу на слайде №24;

• Записать скремблирующую двоичную М-последовательность, порождаемую примитивным многочленом $p(x) = 1+x^2+ x^5$ при начальном состоянии ячеек регистра сдвига из всех «1». Показать, какой станет зашифрованная двоичная последовательность длиной $N = 2^5–1$, состоящая из всех единиц.