ТЕХНОЛОГИИ ОБРАБОТКИ ИНФОРМАЦИИ

ЛЕКЦИЯ 6

ЗАЩИТА ИНФОРМАЦИИ

Что?

Зачем?

Почему?

А надо ли?

Шифрование?

Криптография?

КРИПТОГРАФИЯ

Криптография — это раздел математики, в котором изучаются и разрабатываются системы изменения письма с целью сделать его непонятным для непосвященных лиц.

Простейшая система шифрования — это замена каждого знака письма на другой знак по выбранному правилу.

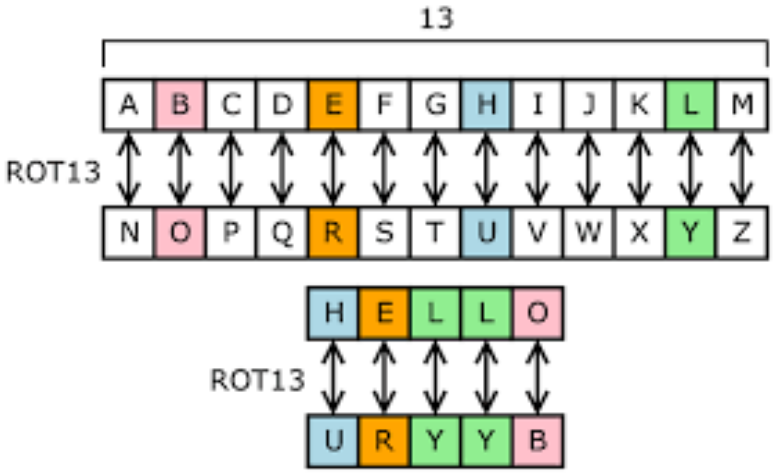
ШИФРЫ И КРИПТОСИСТЕМЫ

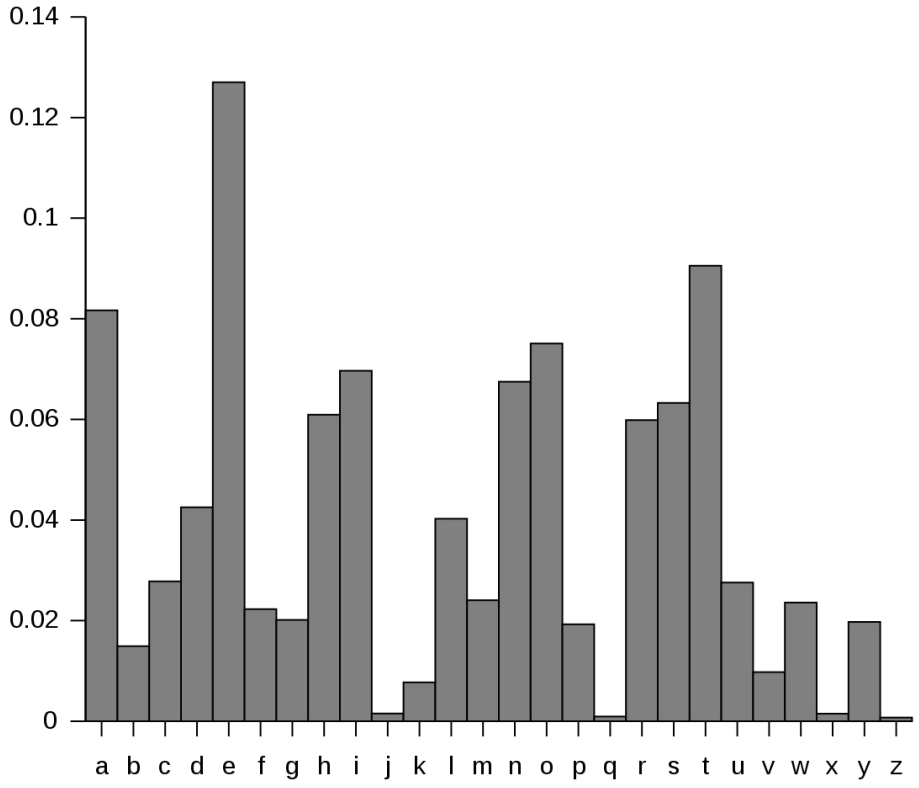
- Шифры простой замены
- Шифры-перестановки
- Симметричное
- Асимметричное шифрование
- Криптосистемы без передачи ключей
- Криптосистемы с открытым ключом
- Электронная подпись

СИММЕТРИЧНЫЕ КРИПТОСИСТЕМЫ

Симметричные криптосистемы - способ шифрования, в котором для шифрования и расшифровывания применяется один и тот же криптографический ключ.

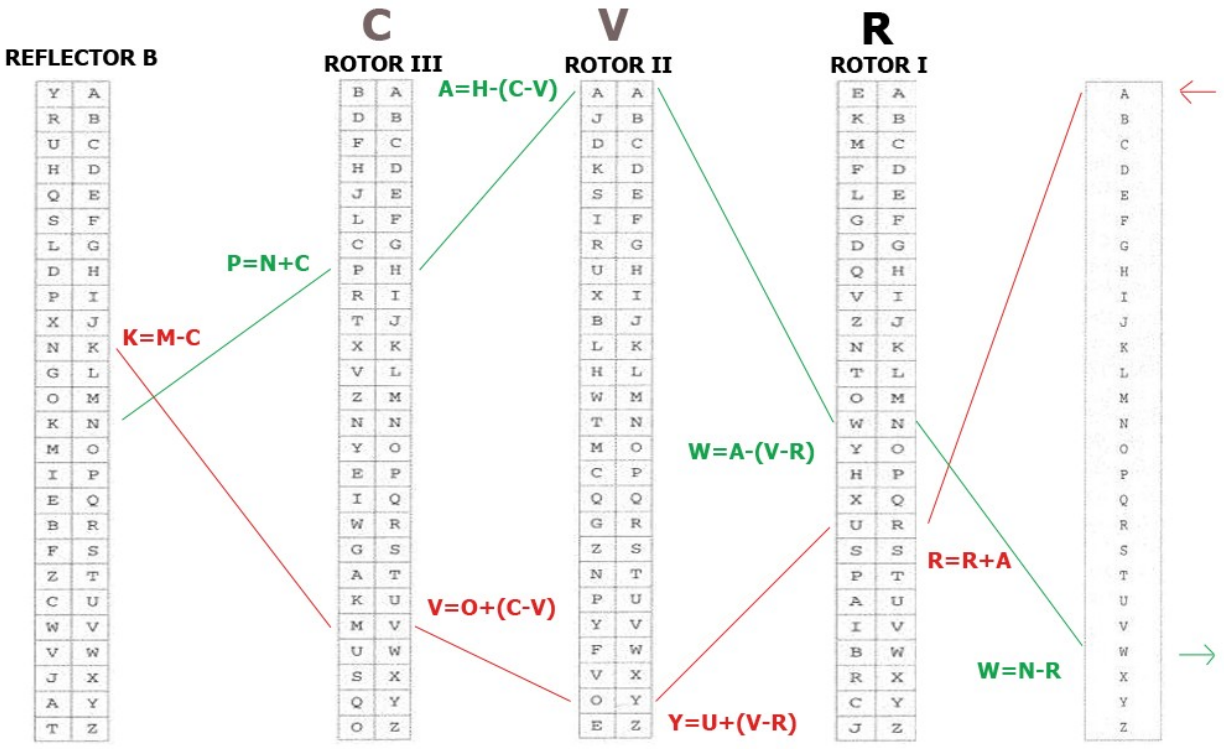
ШИФР ПРОСТОЙ ЗАМЕНЫ





ШИФРЫ-ПЕРЕСТАНОВКИ

ЭНИГМА


REFLECTOR B
C
ROTOR III
V
ROTOR II
R
ROTOR I
A=H-(C-V)
P=N+C
K=M-C
V=O+(C-V)
W=A-(V-R)
R=R+A
W=N-R
Y=U+(V-R)

КРИПТОГРАФИЯ С ОТКРЫТЫМ КЛЮЧОМ

Асимметричное шифрование с открытым ключом базируется на следующих принципах:

- Можно сгенерировать пару очень больших чисел (открытый ключ и закрытый ключ) так, чтобы, зная открытый ключ, нельзя было вычислить закрытый ключ за разумный срок. При этом механизм генерации является общеизвестным.
- Имеются надёжные методы шифрования, позволяющие зашифровать сообщение открытым ключом так, чтобы расшифровать его можно было только закрытым ключом. Механизм шифрования является общеизвестным.
- Владелец двух ключей никому не сообщает закрытый ключ, но передает открытый ключ контрагентам или делает его общеизвестным.

КРИПТОГРАФИЯ С ОТКРЫТЫМ КЛЮЧОМ

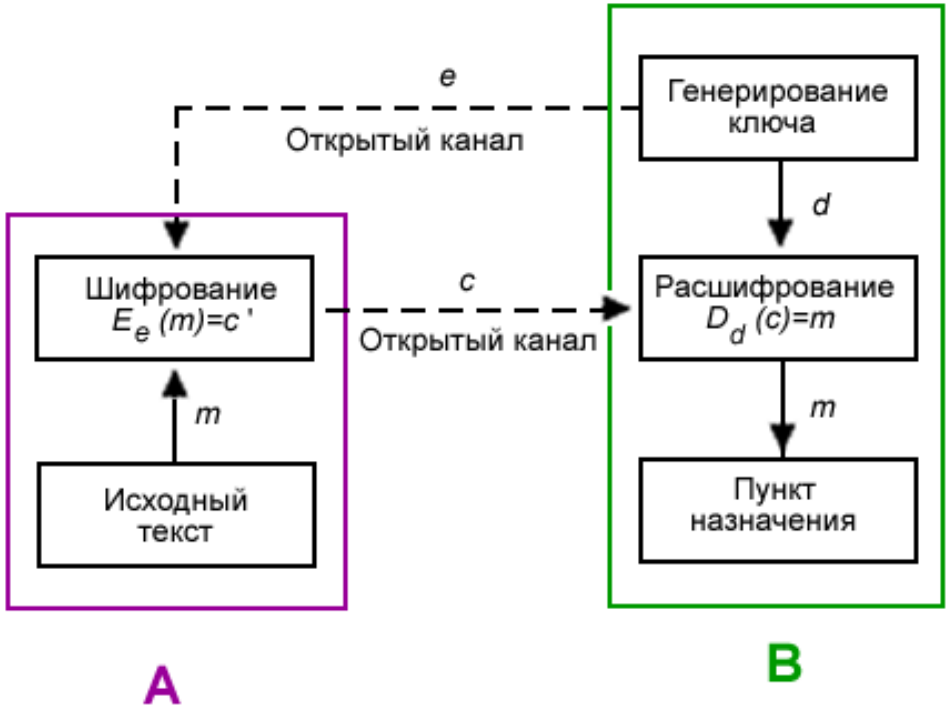
Идея криптографии с открытым ключом очень тесно связана с идеей односторонних функций, то есть таких функций *f(x)*, что по известному *x* довольно просто найти значение *f(x)*, тогда как определение *x* из *f(x)* невозможно за разумный срок.

Имя	f(имя_пароль)
АЛИСА	РОМАШКА
БОБ	НАРЦИСС

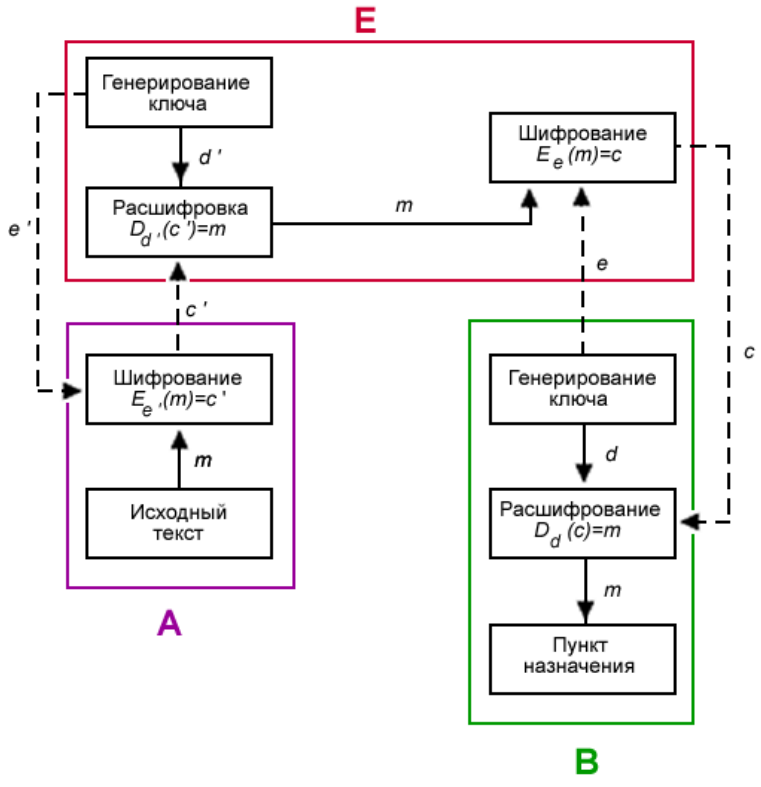
Вход в систему теперь выглядит так:

Имя:	АЛИСА
Пароль:	ГЛАДИОЛУС

СХЕМА ШИФРОВАНИЯ С ОТКРЫТЫМ КЛЮЧОМ



АТАКА НА СИСТЕМУ С ОТКРЫТЫМ КЛЮЧОМ



АЛГОРИТМ ШИФРОВАНИЯ RSA

RSA (аббревиатура от фамилий Rivest, Shamir и Adleman) — криптографический алгоритм с открытым ключом, основывающийся на вычислительной сложности задачи факторизации больших целых чисел.

RSA-ключи генерируются следующим образом:

1) выбираются два различных случайных простых числа p и q заданного размера (например, 1024 бита каждое);

2) вычисляется их произведение $n = pq$, которое называется модулем;

3) вычисляется значение функции Эйлера от числа n: $\varphi(n) = (p-1)(q-1)$

4) выбирается целое число e ($1 < e < \varphi(n)$}1<e<\varphi (n)), взаимно простое со значением функции {\displaystyle \varphi (n)}\varphi (n);

АЛГОРИТМ ШИФРОВАНИЯ RSA

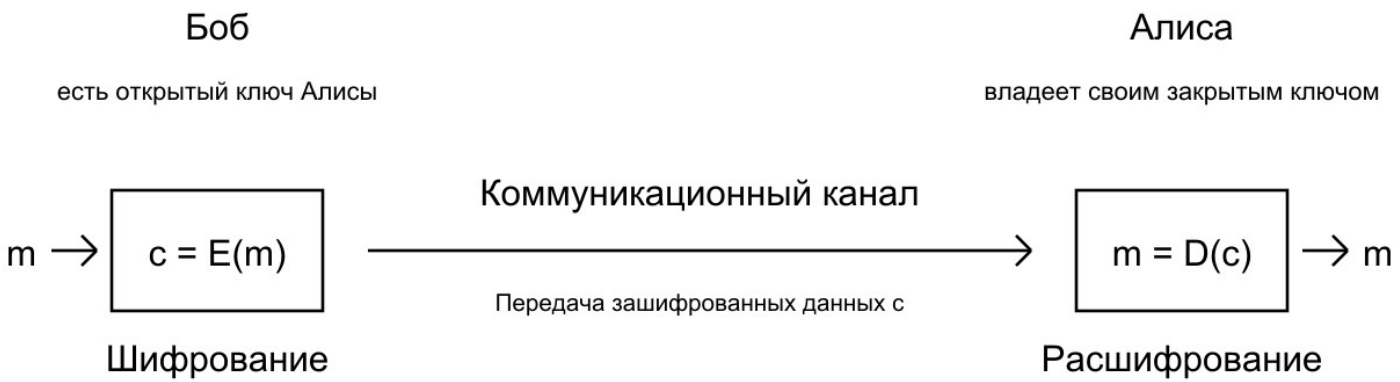
5) вычисляется число d, мультипликативно обратное к числу e по модулю $\varphi(n)$, то есть число, удовлетворяющее сравнению:

$de = 1 \pmod{\varphi(n)}$

6) пара (e,n) публикуется в качестве открытого ключа RSA

7) пара (d,n) играет роль закрытого ключа RSA

ШИФРОВАНИЕ И ДЕШИФРОВАНИЕ



Алгоритм шифрования[16]:

- Взять *открытый ключ* (e, n) Алисы
- Взять *открытый текст* m
- Зашифровать сообщение с использованием открытого ключа Алисы:

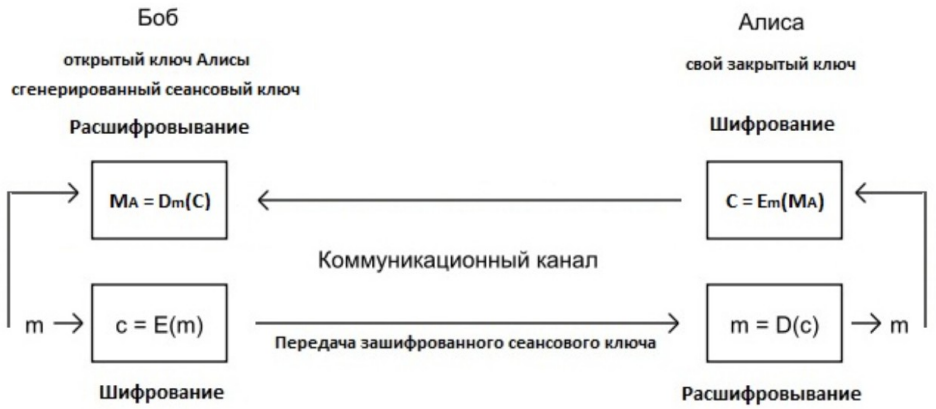
$$c = E(m) = m^e \mod n \quad (1)$$

Алгоритм расшифрования:

- Принять зашифрованное сообщение c
- Взять свой *закрытый ключ* (d, n)
- Применить закрытый ключ для расшифрования сообщения:

$$m = D(c) = c^d \mod n \quad (2)$$

ИСПОЛЬЗОВАНИЕ СЕАНСОВОГО КЛЮЧА



Алгоритм:

- Взять *открытый ключ* (e, n) Алисы
- Создать случайный *сеансовый ключ* m
- Зашифровать сеансовый ключ с использованием открытого ключа Алисы:

$$c = E(m) = m^e \mod n$$

- Расшифровать сообщение C с помощью сеансового ключа симметричным алгоритмом:

$$M_A = D_m(C)$$

Алгоритм:

- Принять зашифрованный сеансовый ключ Боба c
- Взять свой *закрытый ключ* (d, n)
- Применить закрытый ключ для расшифровывания сеансового ключа:

$$m = D(c) = c^d \mod n$$

- Зашифровать сообщение M_A с помощью сеансового ключа симметричным алгоритмом:

$$C = E_m(M_A)$$

ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ

Алгоритм:

- Взять открытый текст m
- Создать цифровую подпись s с помощью своего секретного ключа $\{d, n\}$:
  $s = S_A(m) = m^d \mod n$
- Передать пару $\{m, s\}$, состоящую из сообщения и подписи.

Алгоритм:

- Принять пару $\{m, s\}$
- Взять открытый ключ $\{e, n\}$ Алисы
- Вычислить прообраз сообщения из подписи:
  $m' = P_A(s) = s^e \mod n$
- Проверить подлинность подписи (и неизменность сообщения), сравнив m и m'

Шифрующая файловая система EFS

Encrypting File System (EFS) — система шифрования данных, реализующая шифрование на уровне файлов в операционных системах Microsoft Windows NT. Данная система предоставляет возможность «прозрачного шифрования» данных, хранящихся на разделах с файловой системой NTFS, для защиты потенциально конфиденциальных данных от несанкционированного доступа при физическом доступе к компьютеру и дискам.

EFS использует симметричное шифрование для защиты файлов, а также шифрование. По умолчанию закрытый ключ пользователя защищён с помощью шифрования пользовательским паролем, и защищённость данных зависит от стойкости пароля пользователя.