СЕТИ. КРИПТОГРАФИЯ

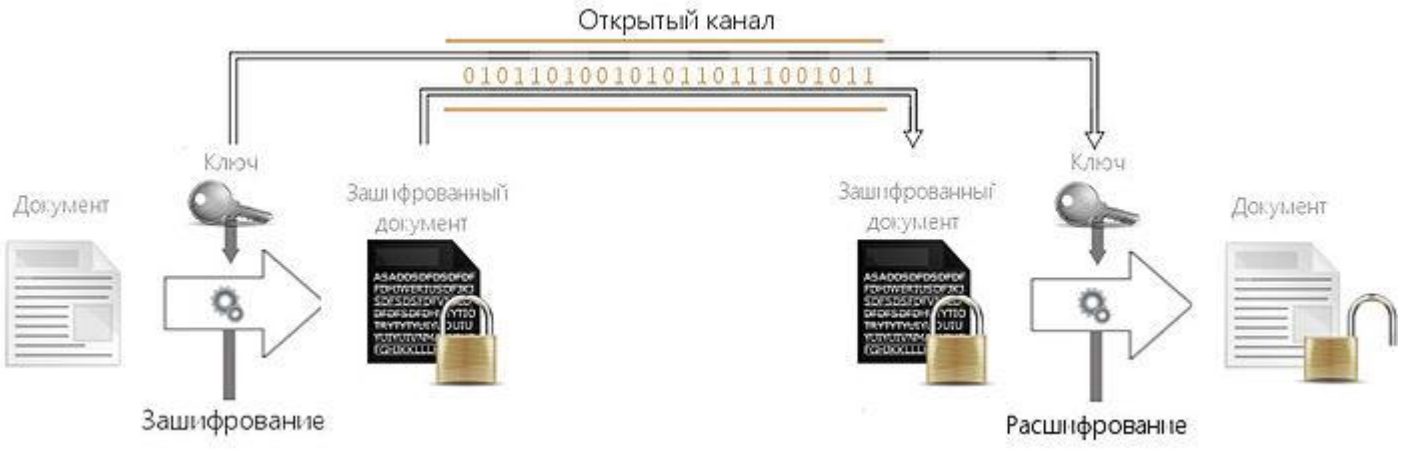
Урок 10. Асимметричное шифрование

С.Ш. и А.Ш.

- Симметричное
  - Простое
  - Быстрое
  - Эффективное
- Ассиметричное
  - Архисложное
  - Долгое
  - Мистическое

Симметричное шифрование

- Решает проблему передачи при наличии закрытого канала



Проблематика

- Нет закрытого канала
- Подмена сообщения
- Подмена пользователя

Односторонние функции

F(x) = A

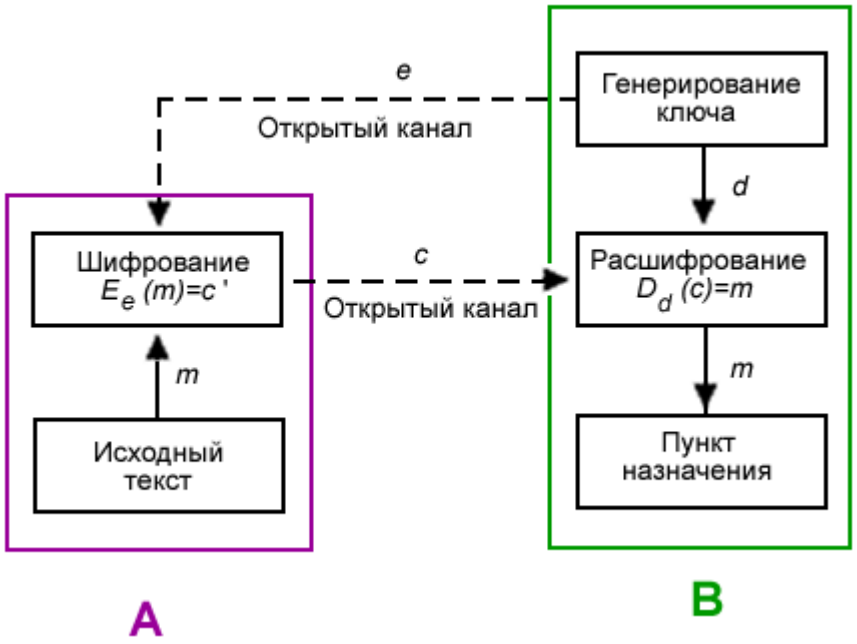
F’(A) = №;%

https://www.youtube.com/watch?v=vFjq9pID4-E

Алгоритм Диффи-Хеллмана

	Алиса	Боб
Этап 1	Оба участника договариваются о значениях **Y** и **P** для общей односторонней функции. Эта информация не является секретной. Допустим были выбраны значения **7** и **11**. Общая функция будет выглядеть следующим образом: 7^X **(mod 11)**	
Этап 2	Алиса выбирает случайное число, например **3**, хранит его в секрете, обозначим его как число **A**	Боб выбирает случайное число, например **6**, хранит его в секрете, обозначим его как число **B**
Этап 3	Алиса подставляет число **A** в общую функцию и вычисляет результат 7^3 **(mod 11)** = 343 (mod 11) = **2**, обозначает результат этого вычисления как число **a**	Боб подставляет число **B** в общую функцию и вычисляет результат 7^6 **(mod 11)** = 117649 (mod 11) = **4**, обозначает результат этого вычисления как число **b**
Этап 4	Алиса передает число **a** Бобу	Боб передает число **b** Алисе
Этап 5	Алиса получает **b** от Боба, и вычисляет значение b^A **(mod 11)** = 4^3 (mod 11) = 64 (mod 11) = **9**	Боб получает **a** от Алисы, и вычисляет значение a^B **(mod 11)** = 2^6 (mod 11) = 64 (mod 11) = **9**
Этап 6	Оба участника в итоге получили число **9**. Это и будет являться ключом.	

RSA - схема


e
Открытый канал
Генерирование ключа
d
Шифрование
$E_e(m)=c'$
c
Открытый канал
Расшифрование
$D_d(c)=m$
m
m
Исходный текст
Пункт назначения
A
B

RSA - математика

Алгоритм RSA состоит из следующих пунктов:

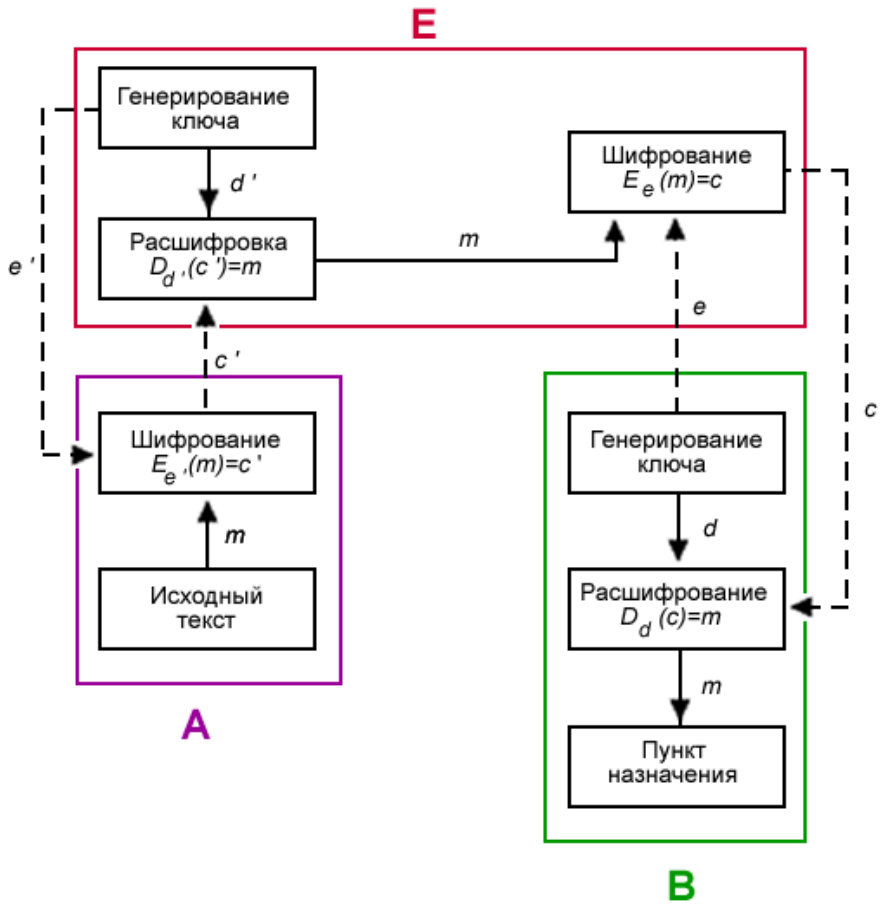
1. Выбрать простые числа p и q
2. Вычислить n = p * q
3. Вычислить f = (p - 1) * (q - 1)
4. Выбрать число d взаимно простое с f
5. Выбрать число e так, чтобы e * d mod f = 1

Числа e и d являются ключами RSA.
Шифруемые данные необходимо разбить на блоки - числа от 0 до n - 1.

Шифрование и дешифровка данных производятся следующим образом:

- Шифрование: $b = a^e \pmod n$
- Дешифровка: $a = b^d \pmod n$

Атака типа «третий посередине»



Сертификаты, Мандаты и ЭЦП