CTF на Физтехе

Занятие 5

Асимметричное шифрование

Асимметричное шифрование

- Для шифрования и расшифровки используются разные ключи
- Открытый ключ известен всем и используется для шифрования
- Закрытый ключ используется для расшифровки
- По открытому ключу нельзя (вычислительно сложно) восстановить закрытый

Протокол Диффи-Хеллмана

Diffie-Hellman Key Exchange

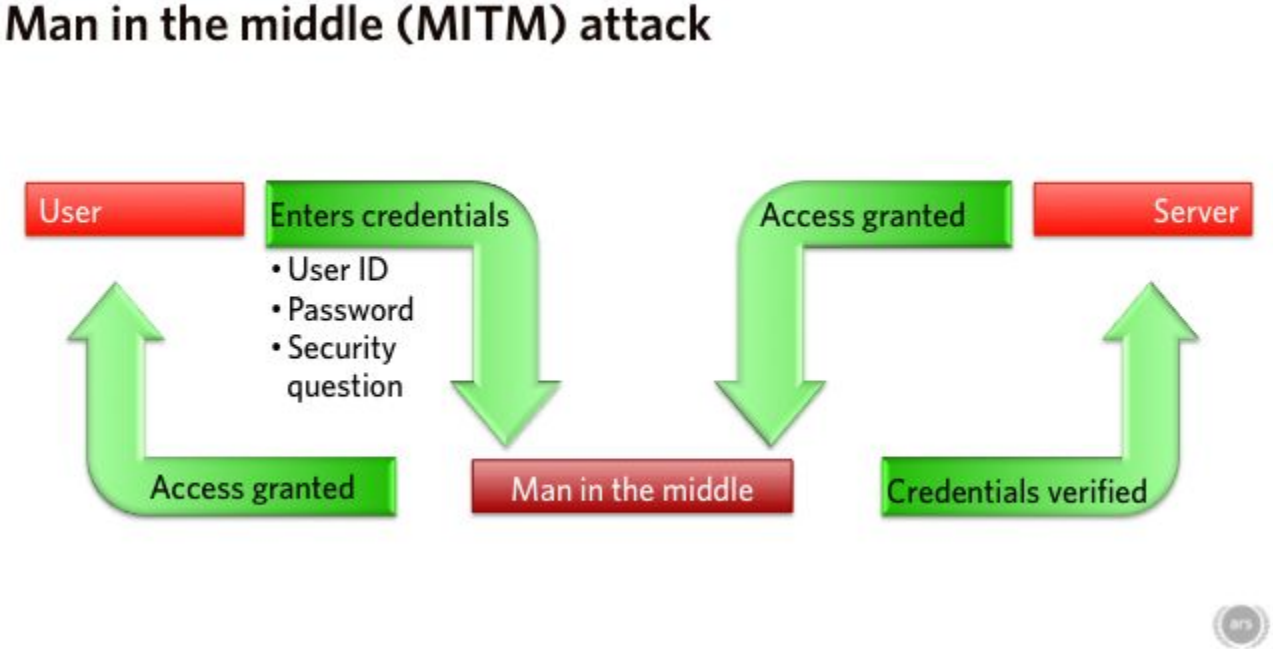
Step	Alice	Bob
1	Parameters: p, g	
2	$A = \text{random}()$ $a = g^A \pmod p$	$\text{random}() = B$ $g^B \pmod p = b$
3	$a \longrightarrow$ $\longleftarrow b$	
4	$K = g^{BA} \pmod p = b^A \pmod p$	$a^B \pmod p = g^{AB} \pmod p = K$
5	$\longleftarrow E_K(data) \longrightarrow$	

Протокол Диффи-Хеллмана: Пример

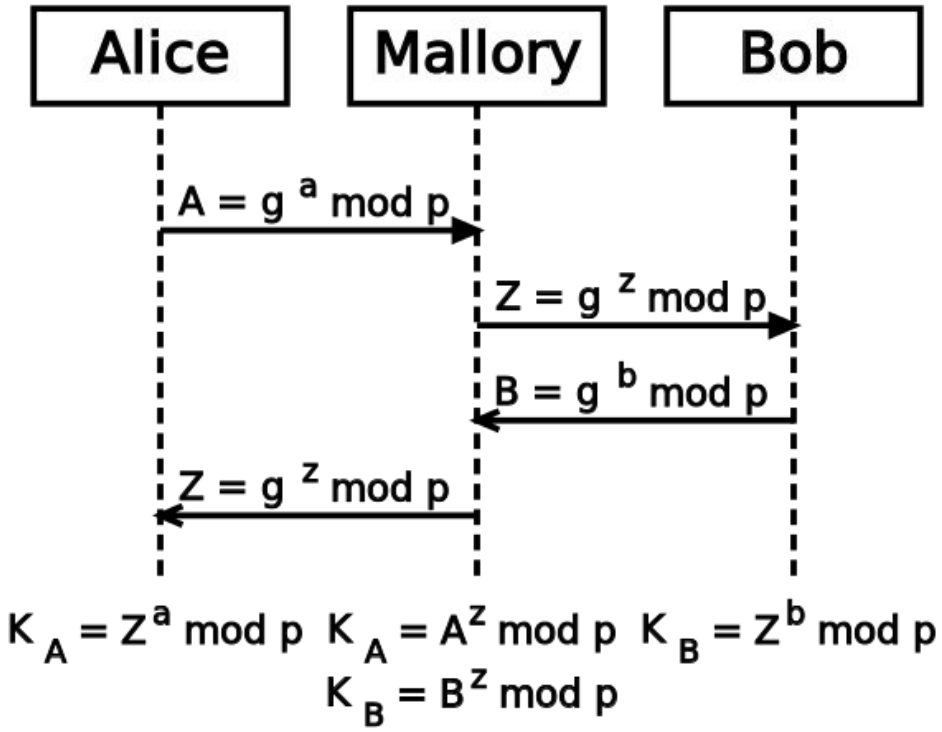
Domain parameters p=29, α=2

Alice		Bob
Choose random private key $k_{prA} = a = 5$		Choose random private key $k_{prB} = b = 12$
Compute corresponding public key $k_{pubA} = A = 2^5 = 3 \bmod 29$	A →	
	← B	Compute correspondig public key $k_{pubB} = B = 2^{12} = 7 \bmod 29$
Compute common secret $k_{AB} = B^a = 7^5 = 16 \bmod 29$		Compute common secret $k_{AB} = A^b = 3^{12} = 16 \bmod 29$

Атака Man-In-The-Middle



Протокол Диффи-Хеллмана: Атака Man-In-The-Middle



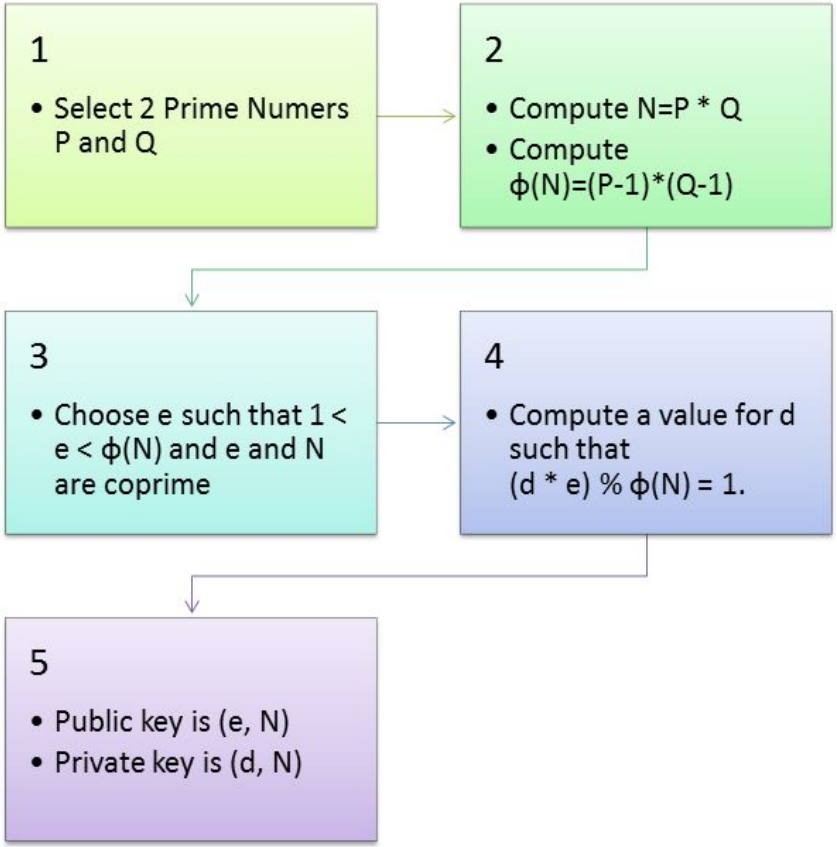
Протокол Диффи-Хеллмана на практике

- Для задачи дискретного логарифмирования нет известного эффективного решения
  - При правильной реализации

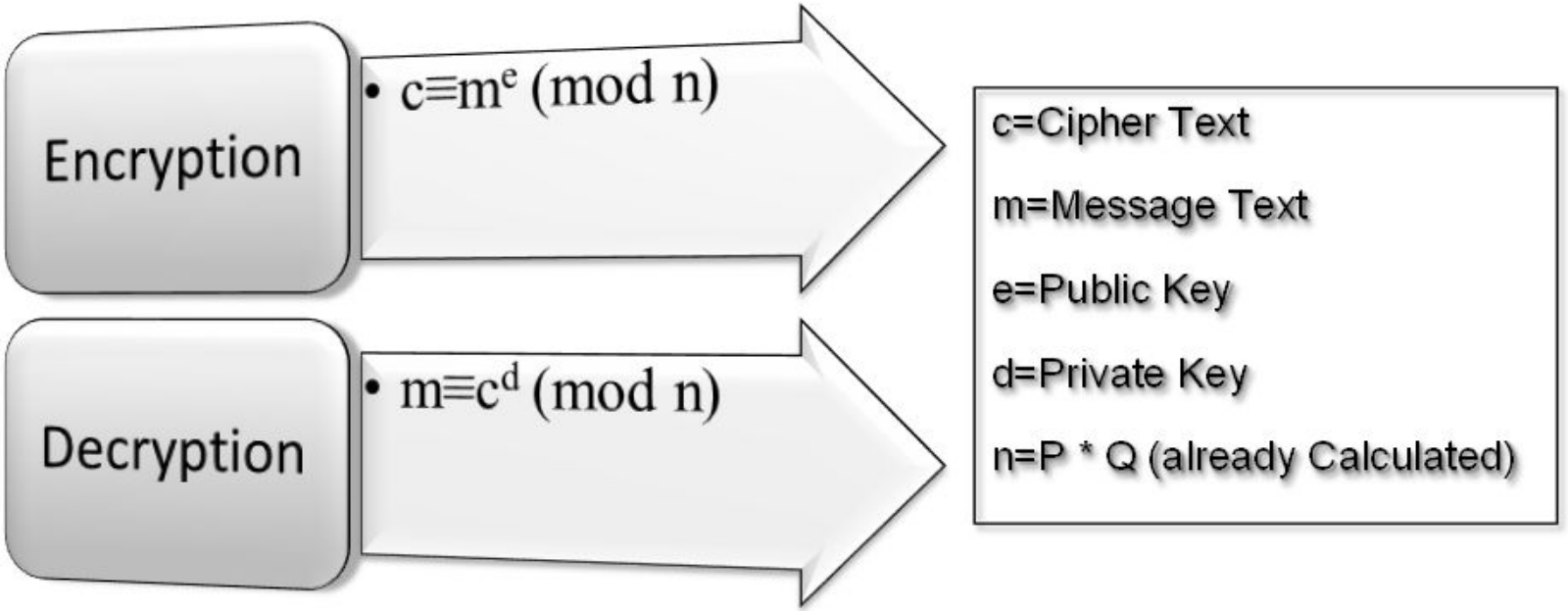
- Для конкретного простого числа p длиной 512 бит
  - Неделя предпосчета на тысячах CPU
  - Минута для решения задачи дискретного логарифмирования на 36 CPU
- Для конретного простого числа p длиной 1024 бит
  - Можно построить систему для взлома DH имея достаточный бюджет (~100kk $)

- Использования простых чисел длиной 2048 бит и больше считается безопасным

RSA


1
• Select 2 Prime Numers P and Q
2
• Compute N=P * Q
• Compute ϕ(N)=(P-1)*(Q-1)
3
• Choose e such that 1 < e < ϕ(N) and e and N are coprime
4
• Compute a value for d such that (d * e) % ϕ(N) = 1.
5
• Public key is (e, N)
• Private key is (d, N)

RSA


Encryption
• $c \equiv m^e \pmod{n}$
Decryption
• $m \equiv c^d \pmod{n}$
c=Cipher Text
m=Message Text
e=Public Key
d=Private Key
n=P * Q (already Calculated)

RSA на практике

- Для задачи факторизации нет известного эффективного решения
  - При правильной реализации

- Для конкретного числа N длиной 512 бит
  - Успешная факторизация за 73 дня на обычной машине в 2009 году
- Самое длинное факторизованное число имеет длину 768 бит
  - Потребовалось 2 года реального времени
  - Известно как RSA-768 в RSA Factoring Challenge

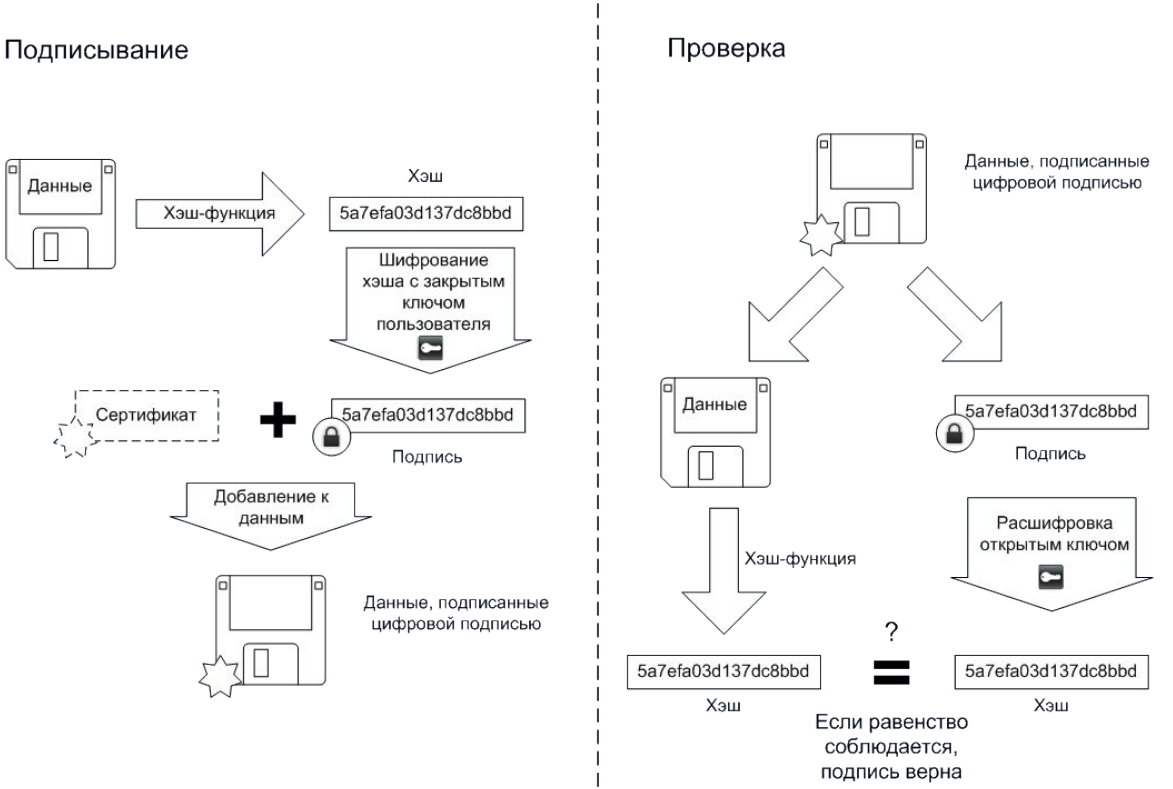
- В теории разложение чисел длиной 1024 скоро будет возможно
- Использования чисел длиной 2048 бит и больше считается безопасным


ВООБРАЖЕНИЕ КРИПТОМАНЬЯКА:
НА ЕГО НОУТЕ ВСЁ ЗАШИФРОВАНО! ДАВАЙ ПОСТРОИМ КЛАСТЕР ЗА МИЛЛИОН ДОЛЛАРОВ И ВСЁ ВЗЛОМАЕМ.
НЕ ВЫЙДЕТ – ТАМ 4096-БИТНЫЙ RSA!
ЧЁРТ! НАШ КОВАРНЫЙ ПЛАН СОРВАН!
ЧТО ПРОИЗОШЛО БЫ В РЕАЛЬНОСТИ:
НА ЕГО НОУТЕ ВСЁ ЗАШИФРОВАНО. ДАЙ ЕМУ НАРКОТЫ И ДУБАСЬ ЭТИМ ГАЕЧНЫМ КЛЮЧОМ ЗА 5 БАКСОВ, ПОКА ОН НЕ СКАЖЕТ ПАРОЛЬ.
ПОНЯЛ.

DH & RSA

- Протокол Диффи-Хеллмана
  - Полагается на отсутствие эффективного решения у задачи дискретного логарифмирования
  - Используется для генерации общего секретного ключа
  - Далее общий ключ обычно используется для шифрования с помощью какого-нибудь алгоритма симетричного шифрования (например AES)
- RSA
  - Полагается на отсутствие эффективного решения у задачи факторизации
  - Используется для генерации закрытого и открытого ключа
  - Далее эти ключи обычно используются для
    - передачи ключа для какого-нибудь алгоритма симметричного шифрования
    - или электронной цифровой подписи

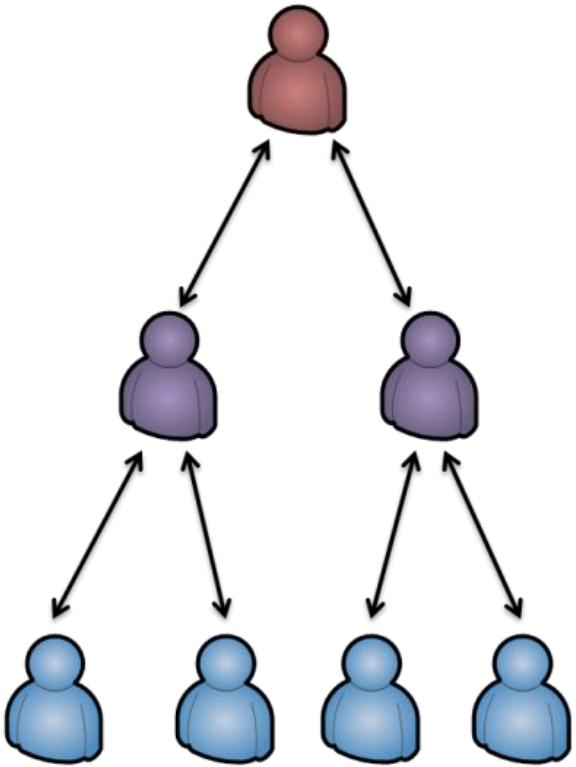
Электронная цифровая подпись



Сертификат открытого ключа

- https://upload.wikimedia.org/wikipedia/commons/9/96/Usage-of-Digital-Certificate.svg

Certificate Authorities



Root
Certificate Authority

Intermediate
Certificate Authority

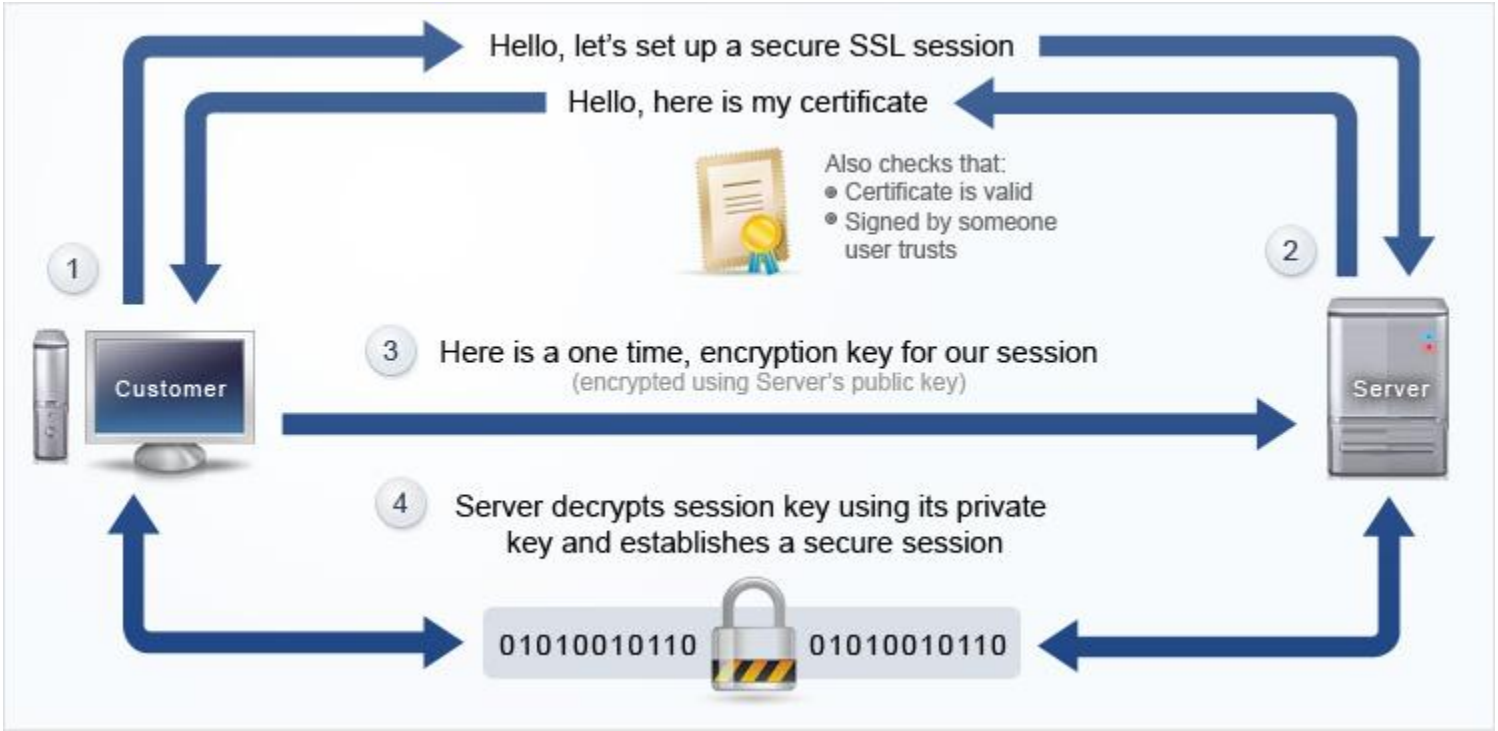
End-User

HTTP vs HTTPS

- Протокол HTTP
  - Используется для получения информации с веб сайтов
  - Небезопасен

- Протокол HTTPS
  - HTTPS = HTTP Secure = HTTP + TLS (SSL)
  - Обеспечивает шифрование
  - Предотвращает Man-In-The-Middle

Как работает HTTPS



HTTPS: Demo

Как получить сертификат

1. Купить
    - от 5$ до 100$ в год

2. Получить бесплатно
    - Let’s Encrypt - открытая бета стартует завтра (3 декабря 2015)

Вопросы?