Ассиметричное шифрование

Определение

Способ шифрования, в котором для шифрования и расшифровывания применяются различные ключи, причём один не может быть простым способом получен из другого.

Открытый и закрытый ключи

- Открытый(публичный) ключ – это ключ, который известен каждому и не является секретной частью алгоритма шифрования. С его помощью, любой желающий может зашифровать сообщение.

- Закрытый ключ – это часть алгоритма, которая является секретной, только обладая этим ключом можно расшифровать сообщение, полученное с помощью открытого ключа и криптографического преобразования.

Другими словами

- Любой желающий может с помощью открытого ключа зашифровать своё послание и отправить его владельцу секретного ключа
- Имеет место следующее преобразование:
  - Сообщение + открытый ключ пользователя = шифртекст
  - Шифртекст + секретный ключ пользователя = сообщение

Односторонняя(вычислительно необратимая функция)

- Функция реализующая преобразование, которое сложно обратить, без знания некоторой секретной информации.

Вариант алгоритма асимметричного шифрования

1. Выбрать два простых числа p и q
2. Вычислить N=p•q
3. Выбрать E, такое, что

$$НОД(E,(p-1)\cdot(q-1))=1$$

4. Найти D, такое, что

$$D=E^{-1}(\mathrm{mod}(p-1)\cdot(q-1))$$

Т.е.

$$D\cdot E=1(\mathrm{mod}(p-1)\cdot(q-1))$$

p	q	N	E	D
Держать в строгом секрете или забыть вовсе	Держать в строгом секрете или забыть вовсе	Держать в общем доступе, для зашифровывания	Держать в общем доступе, для зашифровывания	Держать в строгом секрете

Вариант алгоритма ассиметричного шифрования

- Положим
  - p=7
  - q=11
- Тогда
  - N=77
  - E=13
  - D=37
- Следовательно для зашифровывания числа 8

$$8^{13} (\mathrm{mod}\, 77) = 50$$

- А для расшифровывания

$$50^{37} (\mathrm{mod}\, 77) = 8$$

Это так, потому что

- Все сравнимые по модулю числа, мы считаем равными друг другу
- При возведении числа в степени в степень, степени умножаются

$$(2^2)^3 = (4)^3 = 64 = (2^2)^3 = 2^{2\cdot 3} = 2^6 = 64$$

- Произведение числа с обратным ему, в кольце вычетов даёт 1
- Следовательно

$$m^e = m^e \pmod N$$

$$(m^e)^d = m^{e\cdot d} = m^{e\cdot d} \pmod N = m^1$$

В чём проблема

- Эффективность такого рода алгоритмов базируется на сложности некоторых математических проблем, так в данном случае эксплуатируется сложность разложения числа на простые множители.
- В тоже время перемножение двух простых чисел для получения числа N не представляется сложной задачей
- Без знания p и q не возможно найти обратное(«d») к известному «e», т.к. зная «e» можно вычислить обратное к нему, только зная модуль, а он в свою очередь равен (p-1)•(q-1), найти это значение, можно только зная p и q, но чтобы их найти, надо разложить N на простые множители

Экскурс в прошлое(или откуда (p-1)•(q-1))

- Число элементов кольца вычетов взаимнопростых с модулем, даётся ф-ей Эйлера $\varphi(N)$
- По аналогии с Малой теоремой Ферма, теорема Лагранжа в частности позволяет нам утверждать, что

$$N = p \cdot q$$

$$\varphi(N) = (p-1) \cdot (q-1)$$

$$e^{(p-1)\cdot(q-1)-1} = e^{-1} \bmod((p-1) \cdot (q-1))$$

Как происходит шифрование

- Открытый текст разбивается на блоки длинны меньше N
- Например текст «crypt» можно разбить так

c	r	y	p	t
3	18	25	16	20

- Каждый блок зашифровывается по вышеописанной схеме, т.е.

N=77	E=13	D=37
Модуль	Открытый ключ	Закрытый ключ

- Первые два(N,E) известны всем, D - хранится в тайне

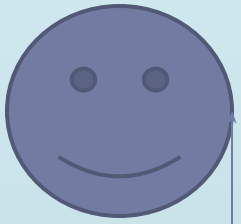
Процедура шифрования

C	3	$3^{13}(\text{mod } 77)$	38
R	18	$18^{13}(\text{mod } 77)$	46
Y	25	$25^{13}(\text{mod } 77)$	60
P	16	$16^{13}(\text{mod } 77)$	37
T	20	$20^{13}(\text{mod } 77)$	69
Итоговое сообщение		{38,46,60,37,69}	

Процедура расшифровывания

38	$38^{37}(\mod 77)$	3	C
46	$46^{37}(\mod 77)$	18	R
60	$60^{37}(\mod 77)$	25	Y
37	$37^{37}(\mod 77)$	16	P
69	$69^{37}(\mod 77)$	20	T
Итоговое сообщение		{C,R,Y,P,T}	

Как выглядит переписка при использовании шифрования с закрытым ключом

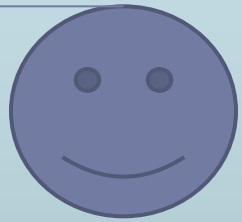


А Алиса расшифрует его ответ своим закрытым ключом

Алиса

Сообщение зашифрованное открытым ключом Боба

Потом он зашифрует ответ для Алисы, её открытым ключом

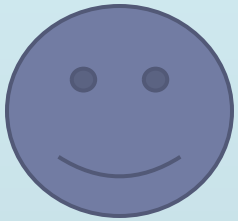


Алиса и Боб обменяются открытыми ключами по не защищённому каналу

Боб

У себя на компьютере Боб расшифрует его своим закрытым ключом и прочтёт

Как работает ЭЦП



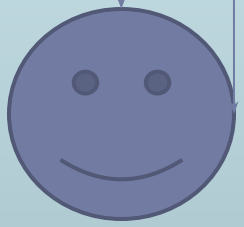
В данном случае закрытый ключ используется для зашифровывания, а открытый для расшифровывания

Алиса

Её важный документ

ХЭШ её важного документа

Зашифрованный Алисиным закрытым ключом ХЭШ



Боб

Боб расшифрует ХЭШ документа открытым ключом Алисы, а потом вычислит ХЭШ документа, который пришёл вместе с зашифрованным. Если значения ХЭШ функций совпадут, БОБ может быть уверен в подлинности документа.

Знать

- Что такое вычислительно необратимые ф-и
- Что такое ассиметричное шифрование
- Что такое закрытый и открытый ключи
- Знать приведённый в презентации примитив RSA
- Уметь объяснять почему это работает
- Знать как происходит процесс шифрования
- Уметь строить простые примеры зашифровывания аналогичные приведённым в презентации

Атаки на симметричные шифры

- В нашем примере длинна ключа не могла превысить

$$2^6 = 64 < N = 77 > 2^7 = 128$$

- Т.е. ключ представляется 7 битами, в свою очередь длинна шифруемого блока не могла превышать 6 бит.