Криптография с открытым ключом

История систем с открытым ключом

- Идея криптографии с открытым ключом впервые появилась в 1976 г. в революционной работе Диффи и Хеллмана «Новые направления в криптографии».

История систем с открытым ключом

- Но только год спустя была опубликована первая (и наиболее успешная) криптосистема с открытым ключом, а именно, *RSA.*



История систем с открытым ключом

- Однако в конце 1990-ых годов выяснилось, что в 1969 году, более чем за пять лет до публикации основополагающей работы Диффи и Хеллмана, Джеймс Эллис, работающий на центр связи Британского правительства (GCHQ), открыл концепцию криптографии с открытым ключом (или несекретное шифрование, как он ее называл) как средство решения проблемы распределения ключей.

История систем с открытым ключом

- Проблема создания работающего алгоритма шифрования с открытым ключом была решена новым сотрудником GCHQ по имени Клиффорд Кокс в 1973 году. В течение одного дня Кокс разработал систему, которая по существу, является алгоритмом *RSA,* за четыре года до Ривеста, Шамира и Адлемана. В 1974 году другой служащий GCHQ, Малькольм Уильямсон, изобрел концепцию алгоритма (обмена ключом) Диффи-Хеллмана.

Слева направо:
Ади Шамир, Рональд Райвист, Леонард Адлеман, Ральф Меркль, Мартин Хеллман, Витфилд Диффи

Основные принципы

- В симметричной криптографии каждая из переписывающихся сторон должна иметь копию общего секретного ключа, что создает сложнейшую проблему управления ключами.
- В криптосистемах с открытым ключом используются два ключа: открытый и секретный.

Основные принципы

- *Открытый ключ* может быть опубликован в справочнике наряду с именем пользователя. В результате любой желающий может зашифровать с его помощью свое письмо и послать закрытую информацию владельцу соответствующего секретного ключа.
- Расшифровать посланное сообщение сможет только тот, у кого есть *секретный ключ*. Более точно, имеют место преобразования:

сообщение + открытый ключ алисы = шифротекст
шифротекст + секретный ключ Алисы = сообщение.

Основные принципы

- Причина работоспособности таких криптосистем: существует односторонняя математическая связь между открытым и секретным ключами, так что:

а) информация об открытом ключе никак не помогает восстановить секретный,

б) владение секретным ключом обеспечивает возможность расшифровывать сообщения, зашифрованные открытым ключом.

Односторонняя функция

- Таким образом, необходимо найти математическое преобразование, которое было бы сложно обратить (без знания специальной секретной информации) на стадии расшифрования.
- Преобразование, обладающее указанным свойством, называется *односторонней функцией* или *функцией-ловушкой,* поскольку в ее дверь войти легко (зашифровать данные), а вот выйти без ключа довольно проблематично.

Односторонние функции (неформальное определение)

- *Односторонней* называется функция $F : X \to Y$ обладающая двумя свойствами:

а) существует полиномиальный алгоритм вычисления значений $F(x)$;

б) не существует полиномиального алгоритма инвертирования функции F (т. е. решения уравнения $F(x) = y$ относительно x,

$$x \in X,\ y \in Y.$$

Вопрос о существовании односторонних функций пока открыт.

Односторонние функции (неформальное определение)

Функцией с секретом k (функция-ловушка) называется функция $F_k : X \to Y,$, зависящая от параметра k и обладающая тремя свойствами:

а) существует полиномиальный алгоритм вычисления значения $F_k(x)$ для любых k и x;

б) не существует полиномиального алгоритма инвертирования F_k при неизвестном k;

в) существует полиномиальный алгоритм инвертирования F_k при известном k.

Примеры односторонних функций

- *Гипотеза о существовании односторонних функций:*

задача разложения целых чисел на множители,

проблема вычисления дискретных логарифмов,

вычисление квадратных корней по модулю составного числа.

- Однако они являются односторонними только в вычислительном отношении, т. е. имея достаточно большие компьютерные мощности, их вполне можно обратить, причем быстрее, чем найти секретный ключ в результате полного перебора.

Применение односторонних функций

- Применение односторонних функций в криптографии позволяет:

организовать обмен шифрованными сообщениями с использованием **только открытых каналов связи**, т. е. отказаться от секретных каналов связи для обмена ключами;

включить в задачу вскрытия шифра трудную математическую задачу и тем самым повысить **обоснованность стойкости шифра**;

решать **новые криптографические задачи**, отличные от шифрования *(электронная цифровая подпись* и др.).

Распределение ключей Диффи-Хеллмана - Меркля

- Протокол позволяет двум сторонам достигнуть соглашения о секретном ключе по открытому каналу связи без предварительной личной встречи. Его стойкость основывается на трудноразрешимой проблеме дискретного логарифмирования в конечной абелевой группе *A.*
- В своей работе авторы предлагали использовать группу *A = GF(p),* но на сегодняшний день многие эффективные версии этого протокола берут за основу группу эллиптической кривой. Такие версии обозначают аббревиатурой *EC-DH,* возникшей от сокращений английских терминов: *Elliptic Curve* и *Diffie-Hellman.* Основные сообщения в протоколе Диффи - Хеллмана представлены следующей диаграммой:

Идея открытого распределения ключей

$$F(x) = \alpha^x \bmod p$$

p - большое простое число, x - произвольное натуральное число, α - некоторый *примитивный элемент* поля $GF(p)$ (числа p и α считаются общедоступными.)

- Известно, что инвертирование функции $\alpha^x \bmod p$, т. е. *дискретное логарифмирование*, является трудной математической задачей.

Идея открытого распределения ключей

- *Протокол выработки общего ключа.*
- Алиса и Боб независимо друг от друга случайно выбирают по одному натуральному числу - скажем a и b. Эти элементы они держат в секрете. Далее каждый из них вычисляет новый элемент: $u = \alpha^a \bmod p$ и $v = \alpha^b \bmod p$.
- Потом они обмениваются этими элементами по каналу связи. Теперь Алиса, получив v и зная свой секретный элемент a, вычисляет новый элемент: $k = v^a = (\alpha^b)^a = \alpha^{ab} \bmod p$

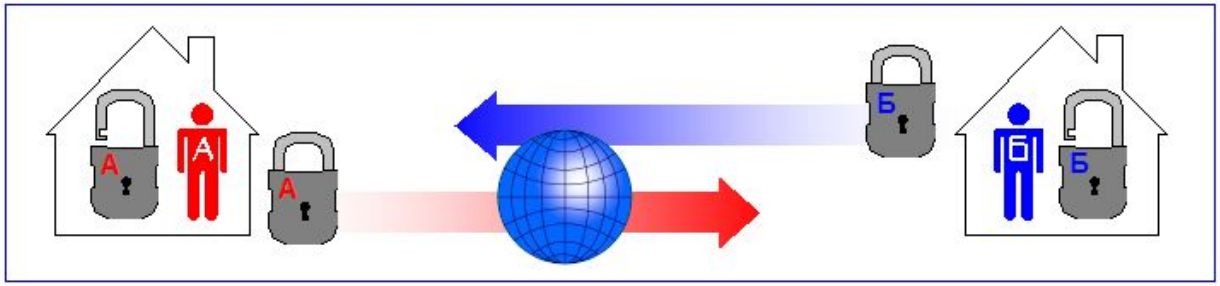
  Аналогично поступает Боб: $k = u^b = (\alpha^a)^b = \alpha^{ab} \bmod p$

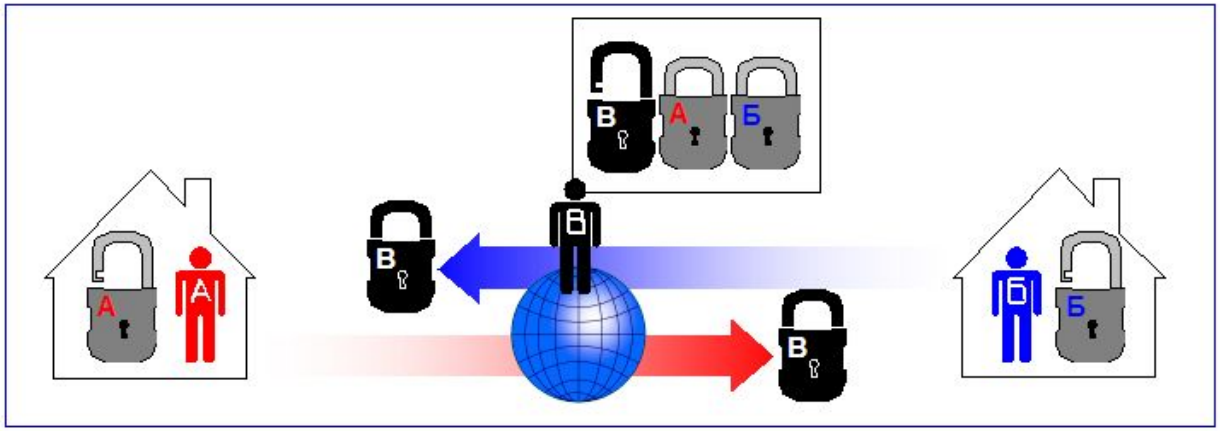
Идея открытого распределения ключей

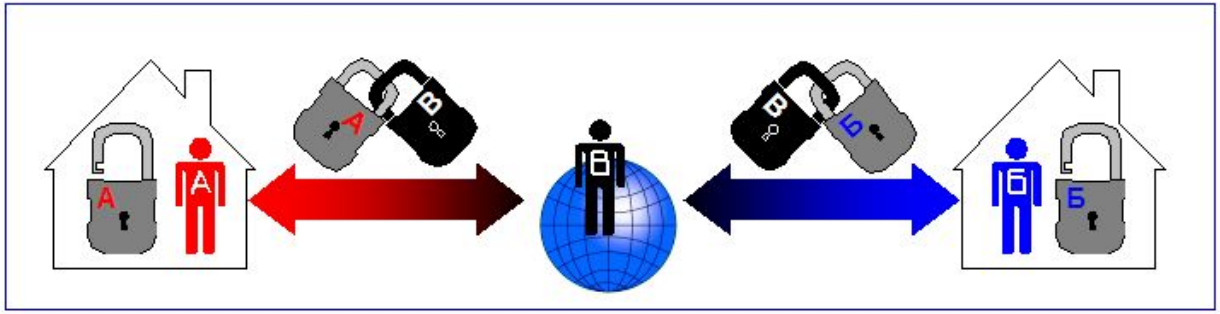
Алиса		*Боб*
a, α^a	$\rightarrow$	α^a
α^b	$\leftarrow$	b, α^b

Алиса вычисляет $k = (\alpha^b)^a = \alpha^{ab} \bmod p$

Боб вычисляет $k = (\alpha^a)^b = \alpha^{ab} \bmod p$


А
А
А
Б
Б
Б


В
А
Б
В
В
А
А
В
Б
Б


А
А
А
В
В
В
Б
Б
Б

Идея открытого распределения ключей (стойкость против пассивного противника)

- Ева может перехватить сообщения, то есть у Евы имеются

$$\alpha, \alpha^a, \alpha^b$$

- Для взлома ключа Еве необходимо вычислить

$$\alpha^{ab}$$

- Поэтому нужно знать $a \quad или \quad b$, а для этого необходимо прологарифмировать

$$\alpha^a или \alpha^b$$

Атака «человек посередине»

Алиса		*Ева*		*Боб*
a	$\rightarrow$	α^a		
α^m	$\leftarrow$	m		
α^{am}		α^{am}		
		n	$\rightarrow$	α^n
		α^b	$\leftarrow$	b
		α^{bn}		α^{bn}

Идея шифрования с открытым ключом

- Алиса хочет получать шифрованные сообщения, поэтому она

выбирает какую-нибудь функцию-ловушку F_k с секретом k,

сообщает всем заинтересованным (например, публикует) описание функции F_k *(открытый ключ)* в качестве своего алгоритма шифрования, но при этом значение секрета k *(закрытый ключ)* она никому не сообщает и держит в секрете

Идея шифрования с открытым ключом

если теперь пользователь Боб хочет послать Алисе защищаемую информацию m , то он вычисляет $c = F_k(m)$ и посылает c по открытому каналу Алисе

Идея шифрования с открытым ключом

поскольку Алиса для своего секрета k умеет инвертировать $F_k(m)$, то она вычисляет m по полученному c. Никто другой не знает k и поэтому в силу свойства функции с секретом не сможет за полиномиальное время по известному шифрованному сообщению вычислить защищаемую информацию m.

Идея цифровой подписи

- Пусть Алисе необходимо подписать сообщение m.

Она, зная секрет k, находит такое s, что $m = F_k(s)$, и вместе с сообщением m посылает s Бобу в качестве своей цифровой подписи.

Подписанное сообщение –пара (m,s)

Идея цифровой подписи

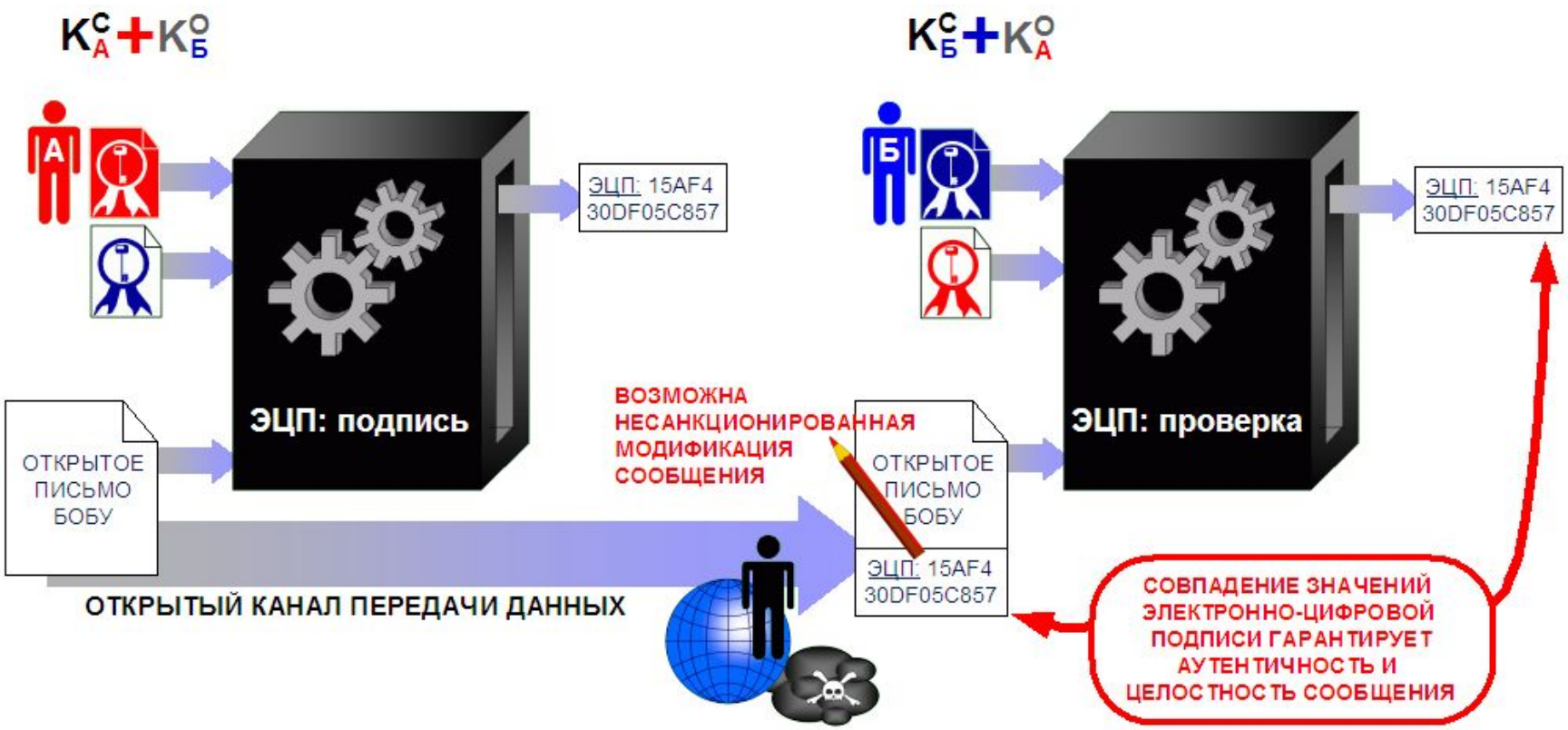
Боб хранит s в качестве доказательства того, что Алиса подписала сообщение m.

Идея цифровой подписи

- Сообщение, подписанное цифровой подписью, можно представлять себе как пару (m, s), где m — сообщение, s — решение уравнения $m = F_k(s)$, где $F_k : M \to S,$ - функция с секретом, известная всем взаимодействующим абонентам.

Свойства цифровой подписи

- Подписать сообщение m (решить ур-е $F_k(s) = m$) может только абонент - обладатель данного секрета k: другими словами, ***подделать подпись невозможно;***


$K_A^C + K_Б^O$
$K_Б^C + K_A^O$
А
Б
ЭЦП: подпись
ЭЦП: проверка
ЭЦП: 15AF4
30DF05C857
ЭЦП: 15AF4
30DF05C857
ОТКРЫТОЕ ПИСЬМО БОБУ
ВОЗМОЖНА НЕСАНКЦИОНИРОВАННАЯ МОДИФИКАЦИЯ СООБЩЕНИЯ
ОТКРЫТОЕ ПИСЬМО БОБУ
ЭЦП: 15AF4
30DF05C857
ОТКРЫТЫЙ КАНАЛ ПЕРЕДАЧИ ДАННЫХ
СОВПАДЕНИЕ ЗНАЧЕНИЙ ЭЛЕКТРОННО-ЦИФРОВОЙ ПОДПИСИ ГАРАНТИРУЕТ АУТЕНТИЧНОСТЬ И ЦЕЛОСТНОСТЬ СООБЩЕНИЯ

Свойства цифровой подписи

- ***проверить подлинность*** подписи может любой абонент, знающий открытый ключ, т. е. саму функцию F_k , для этого проверяется равенство $F_k(s) = m$ при известных s и m

Свойства цифровой подписи

- при возникновении споров ***отказаться от подписи невозможно*** в силу ее неподделываемости;

Свойства цифровой подписи

- подписанные сообщения (m,s) можно, не опасаясь ущерба, пересылать по любым каналам связи.

- Регламентируется законодательством – Федеральный Закон РФ «Об Электронной цифровой подписи» № 1-ФЗ от 10.01.02

Недостатки

- Недостатки:
  - высокие вычислительные затраты
    - решение: применение алгоритмов симметричного шифрования
  - отсутствует прямая возможность аутентификации ключевого обмена
    - атака «Man in the Middle»