Криптографическая система с открытым ключом

(или асимметричное шифрование)

Определение

- система шифрования и/или электронной подписи (ЭП), при которой *открытый ключ* передаётся по открытому (то есть незащищённому, доступному для наблюдения) каналу и используется для проверки ЭП и для шифрования сообщения. Для генерации ЭП и для расшифровки сообщения используется закрытый ключ

- $f(x)$ – одностороння функция
- x – известное значение, с помощью которого, можно вычислить $f(x)$ зная «лазейку» y

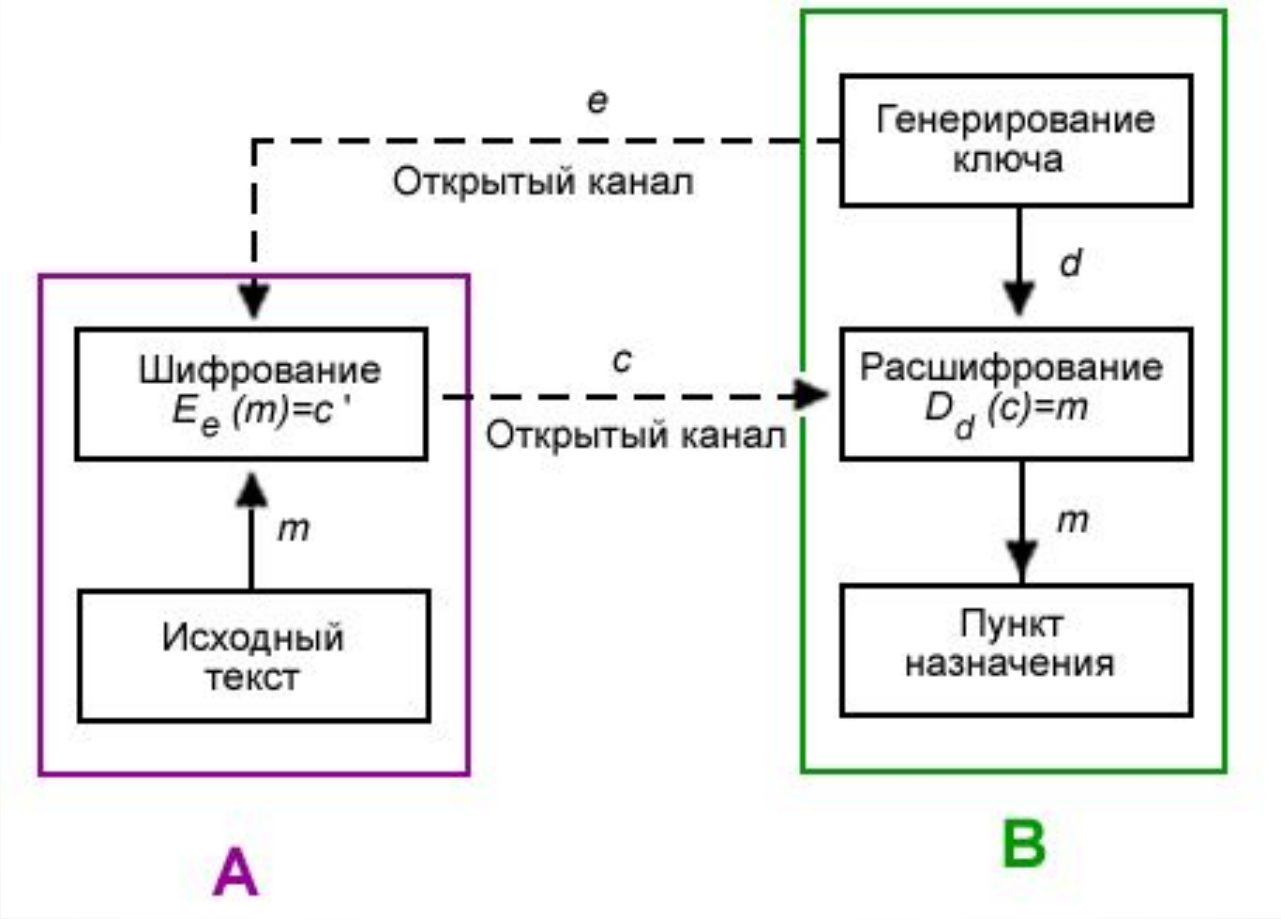
Имя	f(имя_пароль)
АЛИСА	РОМАШКА
БОБ	НАРЦИСС

Имя:	АЛИСА
Пароль:	ГЛАДИОЛУС

Сообщение	Выбранное имя	Криптотекст
К	Королёв	5643452
О	Орехов	3572651
Р	Рузаева	4673956
О	Осипов	3517289
Б	Батурин	7755628
К	Кирсанова	1235267
А	Арсеньева	8492746

Криптотекст 1	Криптотекст 2	Криптотекст 3
1235267	5643452	1235267
3572651	3517289	3517289
4673956	4673956	4673956
3517289	3572651	3572651
7755628	7755628	7755628
5643452	1235267	5643452
8492746	8492746	8492746

Схема шифрования с открытым ключом



Основные принципы построения криптосистем с открытым ключом

- Начинаем с трудной задачи **P**. Она должна решаться сложно в смысле теории: не должно быть алгоритма, с помощью которого можно было бы перебрать все варианты решения задачи **P** за полиномиальное время относительно размера задачи. Более правильно сказать: не должно быть *известного* полиномиального алгоритма, решающего данную задачу — так как ни для одной задачи ещё пока не доказано, что для неё подходящего алгоритма нет в принципе.

Основные принципы построения криптосистем с открытым ключом

- Можно выделить легкую подзадачу **P'** из **P**. Она должна решаться за полиномиальное время и лучше, если за линейное.
- «Перетасовываем и взбалтываем» **P'**, чтобы получить задачу **P''**, совершенно не похожую на первоначальную. Задача **P''** должна по крайней мере выглядеть как оригинальная труднорешаемая задача **P**.

Основные принципы построения криптосистем с открытым ключом

- **P’’** открывается с описанием, как она может быть использована в роли ключа зашифрования. Как из **P’’** получить **P’**, держится в секрете как секретная лазейка.
- Криптосистема организована так, что алгоритмы расшифрования для легального пользователя и криптоаналитика существенно различны. В то время как второй решает **P’’** -задачу, первый использует секретную лазейку и решает **P’** -задачу.

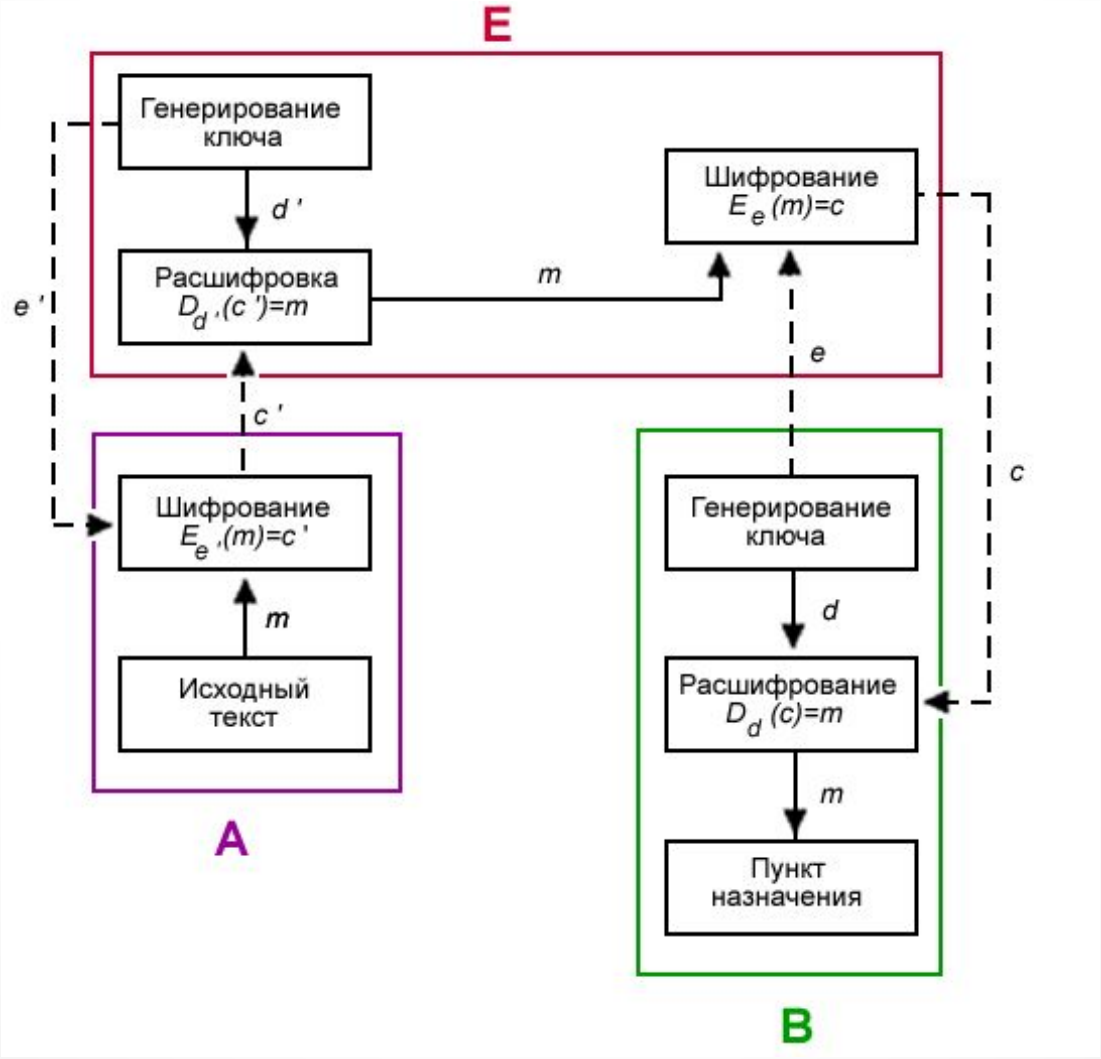
Криптография с несколькими открытыми ключами

Лицо	Ключ
Алиса	K_A
Боб	K_B
Кэрол	K_C
Дэйв	K_A, K_B
Эллен	K_B, K_C
Франк	K_A, K_C

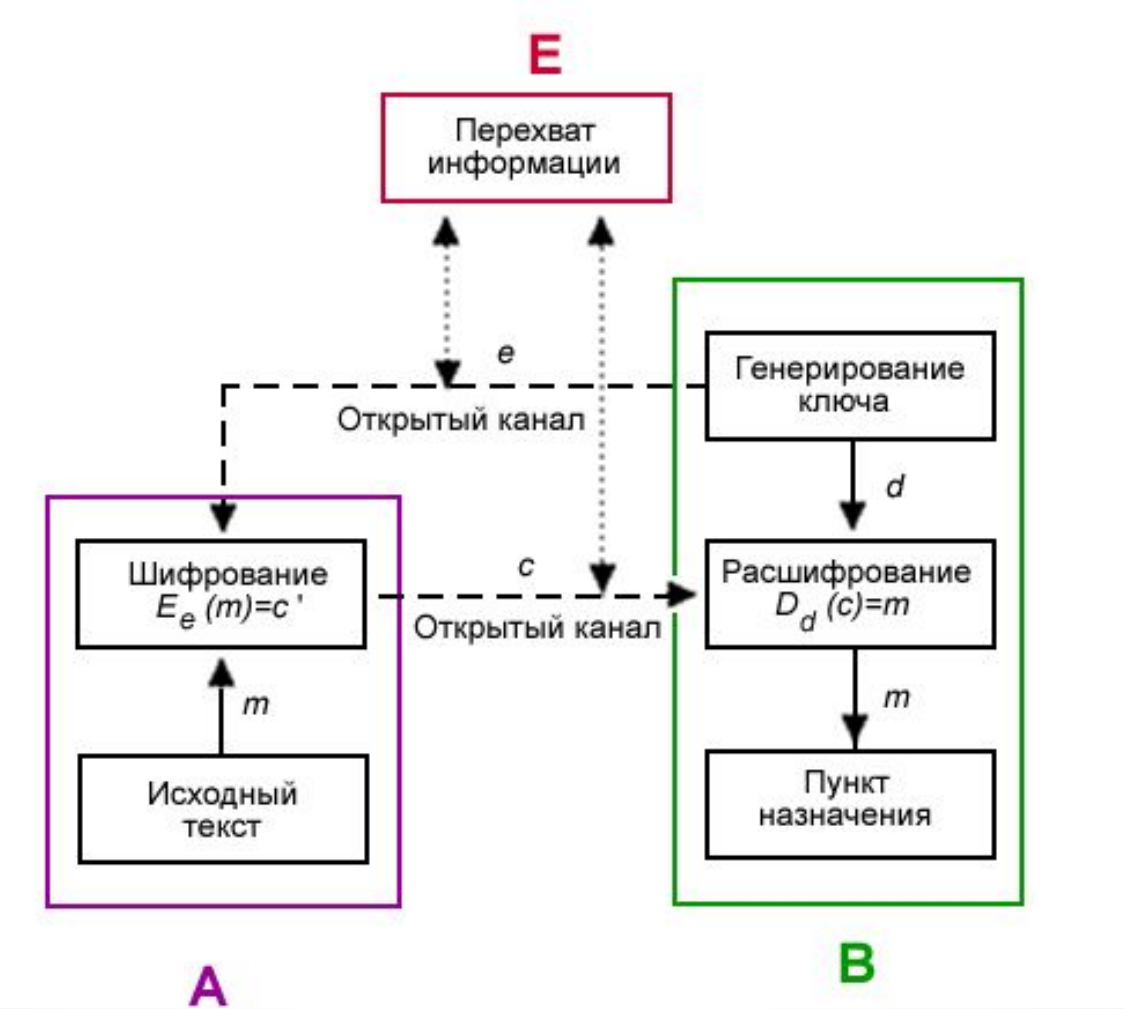
Шифруется ключом	Расшифровывается ключом
K_B и K_C	K_A
K_A и K_C	K_B
K_A и K_B	K_C
K_C	K_A, K_B
K_A	K_B, K_C
K_B	K_A, K_C

- Преимущество этой схемы заключается в том, что для её реализации нужно только одно сообщение и n ключей (в схеме с n агентами).
- Недостатком такой схемы является то, что необходимо также широковещательно передавать подмножество агентов (список имён может быть внушительным), которым нужно передать сообщение.

Криптоанализ алгоритмов с открытым ключом



Криптоанализ алгоритмов с открытым ключом



Применение

Алгоритмы криптосистемы с открытым ключом можно использовать:

- как самостоятельное средство для защиты передаваемой и хранимой информации;
- как средство распределения ключей (обычно с помощью алгоритмов криптосистем с открытым ключом распределяют ключи, малые по объёму, а саму передачу больших информационных потоков осуществляют с помощью других алгоритмов);
- как средство аутентификации пользователей.

Преимущества

- Не нужно предварительно передавать секретный ключ по надёжному каналу.
- Только одной стороне известен ключ дешифрования, который нужно держать в секрете (в симметричной криптографии такой ключ известен обеим сторонам и должен держаться в секрете обеими).
- В больших сетях число ключей в асимметричной криптосистеме значительно меньше, чем в симметричной.

Недостатки

- В алгоритм сложнее внести изменения.
- Более длинные ключи. Ниже приведена таблица, сопоставляющая длину ключа симметричного алгоритма с длиной ключа RSA с аналогичной криптостойкостью:

Длина симметричного ключа, бит	Длина ключа RSA, бит
56	384
64	512
80	768
112	1792
128	2304

Недостатки

- Шифрование-расшифрование с использованием пары ключей проходит на два-три порядка медленнее, чем шифрование-расшифрование того же текста симметричным алгоритмом.
- Требуются существенно бóльшие вычислительные ресурсы, поэтому на практике асимметричные криптосистемы используются в сочетании с другими алгоритмами:
  - Для ЭЦП сообщение предварительно подвергается хешированию, а с помощью асимметричного ключа подписывается лишь относительно небольшой результат хеш-функции.
  - Для шифрования они используются в форме гибридных криптосистем, где большие объёмы данных шифруются симметричным шифром на сеансовом ключе, а с помощью асимметричного шифра передаётся только сам сеансовый ключ.

Ассиметричные шифры. RSA

- 1. Выбираются два различных случайных простых числа p и q заданного размера (например, 1024 бита каждое).
- 2. Вычисляется их произведение $n = p \times q$, которое называется модулем.
- 3. Вычисляется значение функции Эйлера от числа n:

$$\varphi(n) = (p-1) \times (q-1).$$

- Выбирается целое число $e\big(1 < e < \varphi(n)\big)$, взаимно простое со значением функции $\varphi(n)$. Обычно в качестве e берут простые числа, содержащие небольшое количество единичных бит в двоичной записи, например, простые числа Ферма 17, 257 или 65537. Число e называется открытой экспонентой (англ. public exponent). Время, необходимое для шифрования с использованием быстрого возведения в степень, пропорционально числу единичных бит в e. Слишком малые значения e, например, 3, потенциально могут ослабить безопасность схемы RSA.
- Вычисляется число d, мультипликативно обратное к числу e по модулю $\varphi(n)$, то есть число, удовлетворяющее сравнению:
- $d \cdot e \equiv 1 \big(mod\ \varphi(n)\big)$.
- Число d называется секретной экспонентой. Обычно, оно вычисляется при помощи расширенного алгоритма Евклида.
- Пара $\{e, n\}$ публикуется в качестве открытого ключа RSA (англ. RSA public key).
- Пара $\{d, n\}$ играет роль закрытого ключа RSA (англ. RSA private key) и держится в секрете.

Пример работы алгоритма RSA.

Генерация ключа

- Выбираем два просты различных числа:
$$p = 3557, q = 2579$$
- Вычисляем произведение:
$$n = p \times q = 3557 \times 2579 = 9173503$$
- Вычисляем функцию Эйлера:
$$\varphi(n) = (p - 1) \times (q - 1) = 9167368$$
- Выбираем открытую экспоненту:
$$e = 3$$
- Вычисляем секретную экспоненту
$$d = e^{-1} mod\ \varphi(n) \Rightarrow d = 6111579$$
- Публикуем открытый ключ:
$$\{e, n\} = \{3, 9173503\}$$
- Сохраняем закрытый ключ

$$\{d\ n\} = \{6111579, 9173503\}$$

Шифрование

- Сообщение

$$m = 111111$$

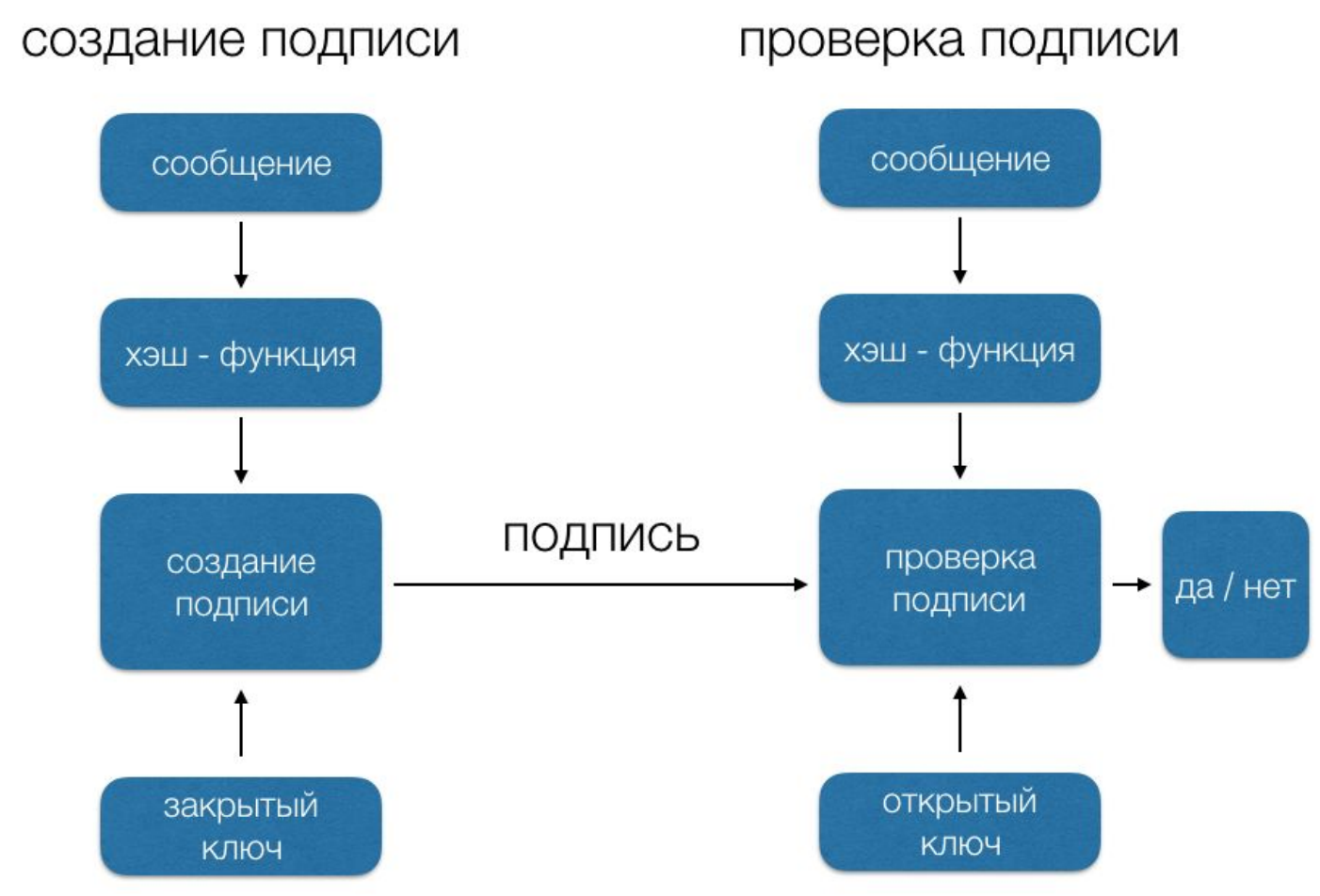
- Вычислить шифртекст

$$c = E(m) = m^e \bmod n =$$
$$= 111111^3 \bmod 9173503 = 4051753$$

- Вычислить исходное сообщение

$$m = D(c) = c^d \bmod n = 4051753^{6111579} \bmod 9173503 =$$
$$= 111111$$

Ассиметричные шифры. DSA



Спасибо за внимание