

Шифрование с открытым КЛЮЧОМ



АЛГОРИТМ RSA



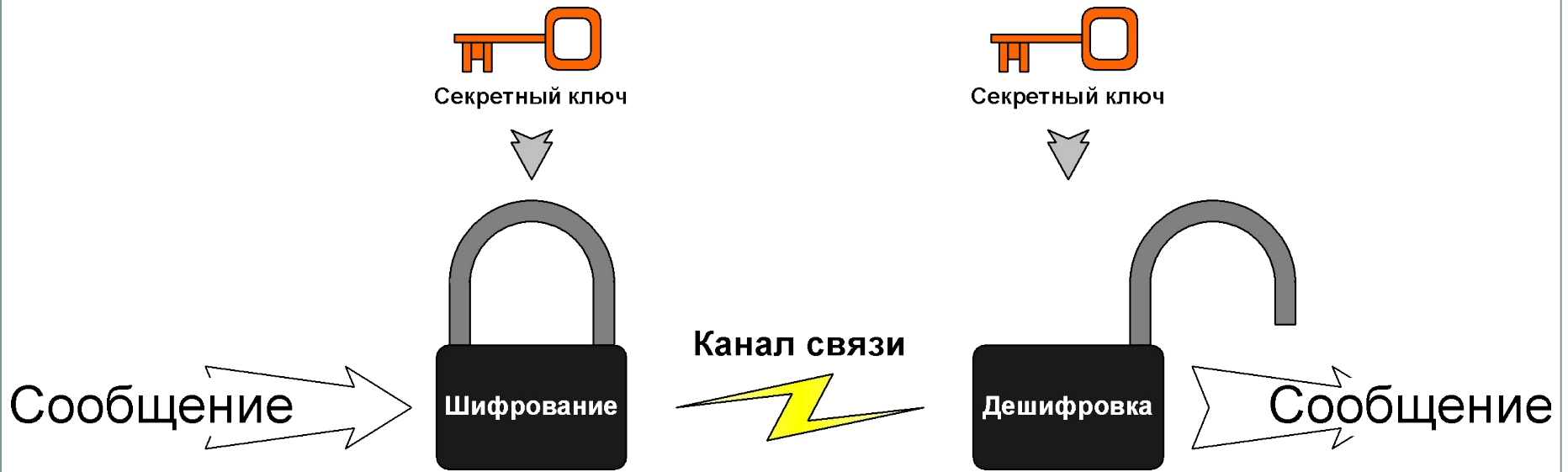
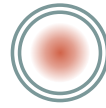
Симметричный шифр



- **Симметричный шифр** – метод передачи шифрованной информации, в котором зашифровывающий и расшифровывающий **ключи совпадают.**
- *Стороны, обменивающиеся зашифрованными данными, должны знать **общий секретный ключ.***



Симметричный шифр





Симметричный шифр



- **Достоинства:**

- Всего один зашифровывающий / расшифровывающий ключ

- **Недостатки:**

- Процесс обмена информацией о секретном ключе представляет собой брешь в безопасности.
- Для передачи секретного ключа необходим закрытый канал связи.

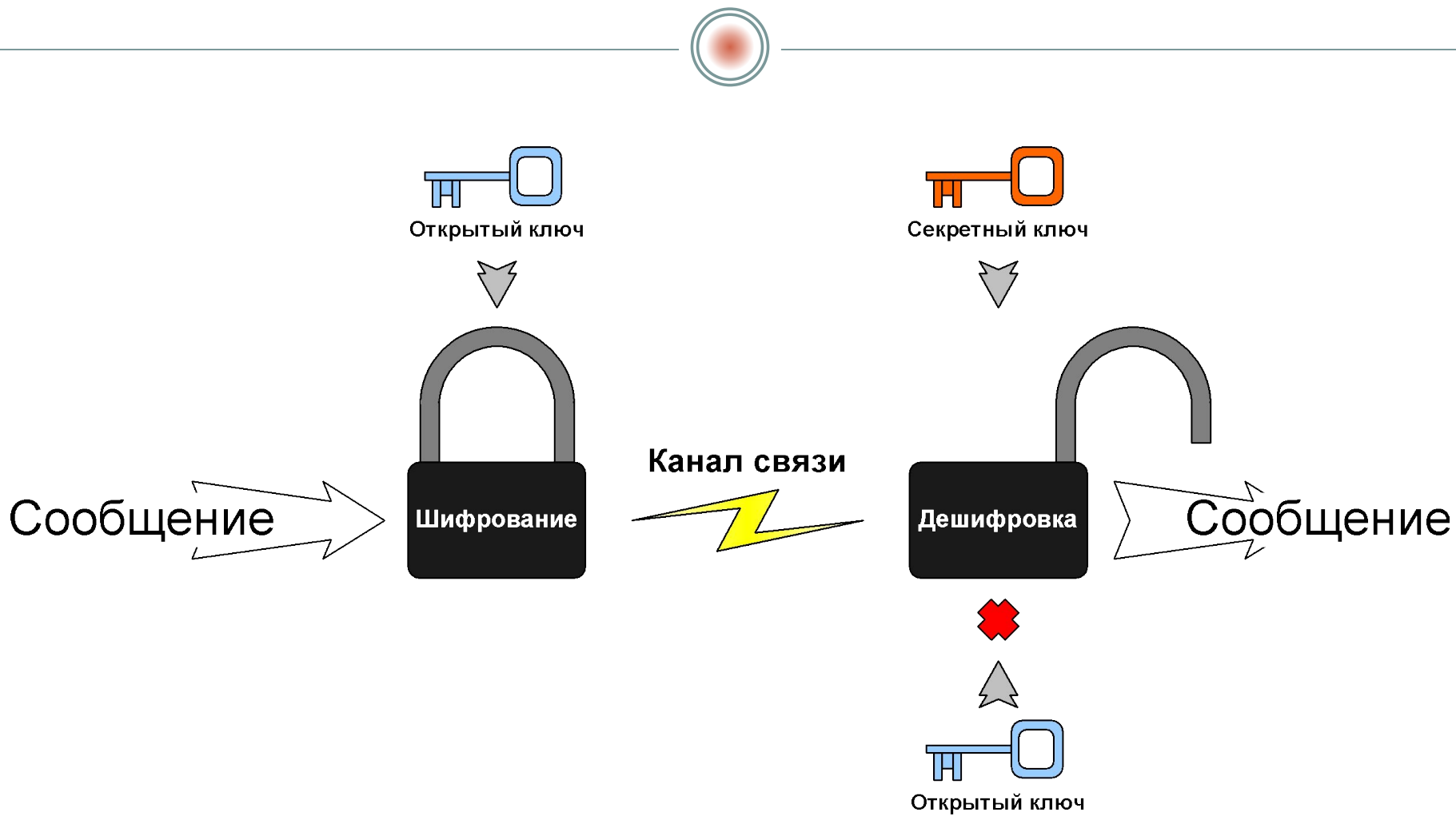


Ассиметричный шифр



- **Ассиметричный шифр** – метод передачи шифрованной информации, в котором зашифровывающий и расшифровывающий **ключи не совпадают**.
- *Ассиметричное шифрование является односторонним процессом.*
- *Данные шифруются только открытым ключом*
- *Расшифровываются только секретным*
- *Открытый и секретный ключ связаны между собой.*

< Ассиметричный шифр





Ассиметричный шифр



● **Достоинства:**

- Для передачи ключа не нужен закрытый канал связи.
- Открытый ключ может быть свободно распространен, это позволяет принимать данные от всех пользователей.

● **Недостатки:**

- Ресурсоемкий алгоритм шифрования / дешифрирования

< Виды асимметричных шифров



- **RSA**
 - Rivest-Shamir-Adleman (Ривест-Шамир-Адлеман)
- **DSA**
 - Digital Signature Algorithm (Алгоритм цифровой подписи)
- **EGSA**
 - El-Gamal Signature Algorithm (Алгоритм ЭЦП Эль-Гамалья)
- **ECC**
 - Elliptic Curve Cryptography (Криптография эллиптической кривой)
- **ГОСТ Р 34.10-94**
 - Российский стандарт схожий с DSA
- **ГОСТ Р 34.10-2001**
 - Российский стандарт схожий с ECC



Алгоритм RSA



- RSA (1977 г.) – криптографическая система открытого ключа. Обеспечивает такие механизмы защиты как шифрование и цифровая подпись.
 - Цифровая подпись (ЭЦП) – механизм аутентификации, позволяющий проверить принадлежность подписи электронного документа его владельцу.
- Алгоритм RSA используется в Internet, к примеру в:
 - S/MIME
 - IPSEC (Internet Protocol Security)
 - TLS (которым предполагается заменить SSL)
 - WAP WTLS.



Алгоритм RSA: Теория



- В основу асимметричных криптосистем кладётся одна из сложных математических проблем, которая позволяет строить односторонние функции и функции-лазейки.
- В основе алгоритма RSA лежит вычислительная проблема разложения больших чисел на простые множители.

Алгоритм RSA: Теория



- Односторонняя функция – функция, которая вычисляется только прямо, т.е. не обращается.
 - Возможно найти $f(x)$, зная x , но невозможно обратное.
- **Односторонней функцией в RSA служит функция для шифрования.**
- Лазейка – некий секрет, зная который можно обратить одностороннюю функцию.
- **Лазейкой в RSA является секретный ключ.**

< Алгоритм RSA: Реализация



1. Выбираются два случайных простых числа p и q заданного размера
 - $p = 3$
 - $q = 11$
2. Вычисляется модуль, n
 - $n = p \cdot q = 33$
3. Вычисляется значение функции Эйлера $\varphi(n)$
 - $\varphi(n) = (p - 1) \cdot (q - 1) = 20$

< Алгоритм RSA: Реализация



4. Выбирается целое число $1 < e < \varphi(n)$ $[1 < e < 20]$
взаимно простое со значением функции $\varphi(n) = 20$
 - $e = 3$
 - e – открытая экспонента
5. Вычисляется число d , мультипликативно обратное к числу e , т.е. $d \cdot e \pmod{\varphi(n)} = 1$
 - $d = 7$
 - d – секретная экспонента
6. Открытый ключ $P = \{e, n\}$
7. Секретный ключ $S = \{d, n\}$

< Алгоритм RSA: Реализация



● Шифрование

- Формула для шифрования $b_i = a_i^e \pmod{n}$
- Возьмем к примеру сообщение $a = \{C, R, Y, P, T, O\}$
- Запишем его кодом в соответствии с алфавитом
 - $a = \{3, 18, 25, 16, 20, 15\}$
- Результат: $b = \{27, 24, 16, 4, 14, 9\}$
- Пример: $16 = 25^3 + 473 \cdot 33$

$$27 = 3^3 \pmod{33}$$

$$4 = 16^3 \pmod{33}$$

$$24 = 18^3 \pmod{33}$$

$$14 = 20^3 \pmod{33}$$

$$16 = 25^3 \pmod{33}$$

$$9 = 15^3 \pmod{33}$$

< Алгоритм RSA: Реализация



● Дешифрирование

- Формула для дешифрования $a_i = b_i^d \pmod{n}$
- Шифрованное сообщение $b = \{27, 24, 16, 4, 14, 9\}$
- Результат: $a = \{3, 18, 25, 16, 20, 15\}$
- В соответствии с алфавитом: $a = \{C, R, Y, P, T, O\}$
- Пример: $25 = 16^7 + 8134407 \cdot 33$

$$3 = 27^7 \pmod{33}$$

$$16 = 4^7 \pmod{33}$$

$$18 = 24^7 \pmod{33}$$

$$20 = 14^7 \pmod{33}$$

$$25 = 16^7 \pmod{33}$$

$$15 = 9^7 \pmod{33}$$



Заключение



- Алгоритмы асимметричного шифрования используют как вспомогательный инструмент для передачи небольших объемов информации, к примеру секретных ключей симметричного шифра.
- Такие гибридные системы получили широкое распространение и классический алгоритм RSA сейчас является частью множества других безопасных протоколов передачи данных.