[IS] Основы информационной безопасности

Современная криптография

Занятие 5

Алгоритмы шифрования

Симметричные и ассиметричные

Алгоритмы шифрования

Симметричные используют один и тот же ключ для шифрования и расшифровывания

Алгоритмы шифрования

У асимметричных есть два ключа: открытый и закрытый, один для шифрования, другой для расшифровывания

Виды шифров

Поточный шифр - каждый байт шифруется отдельно

Блочный шифр - шифруется фрагмент из нескольких байтов

Есть сообщение, которое нужно зашифровать “task”. Есть ключ “ctf”. Как же мы можем это сделать?

XOR

$\oplus$

$0 \oplus 0 = 0$

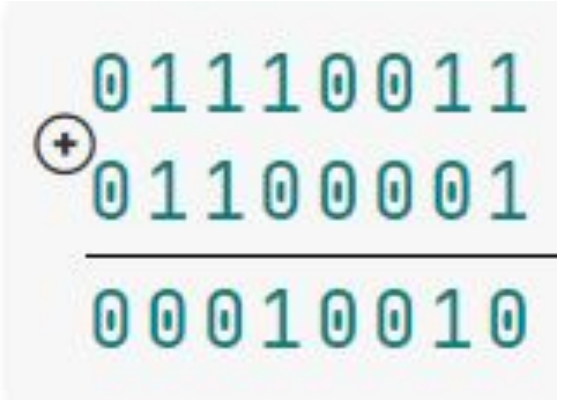
$0 \oplus 1 = 1$

$1 \oplus 0 = 1$

$1 \oplus 1 = 0$

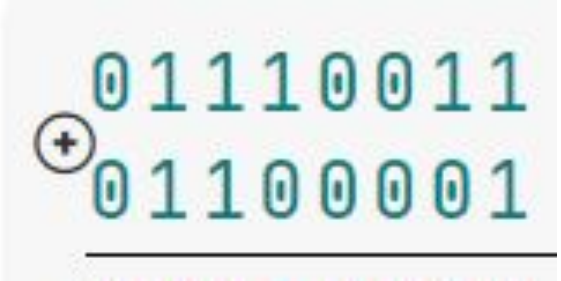
XOR

$$A \oplus B \oplus B = A$$



XOR

1. Подгоняем длину ключа под длину текста
2. Преобразовываем текст и ключ в двоичное представление
3. 3. Вычисляем XOR побитно



XOR

Абсолютная криптографическая стойкость — имея шифротекст без ключа, невозможно получить никакую информацию об исходном тексте

XOR

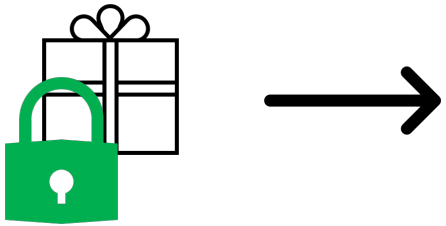
У злоумышленника тексты $X = A \oplus K$ и $Y = B \oplus K$

Он посчитает $X \oplus Y$, то получит $A \oplus K \oplus B \oplus K$

Но $K \oplus K = 0$, а значит, $X \oplus Y = A \oplus B$

Как отправить посылку, чтобы никто третий ее не открыл?

Алиса
замок с ключом

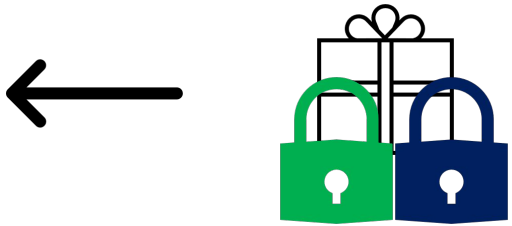


Боб
замок с ключом

Как отправить посылку, чтобы никто третий ее не открыл?

Алиса
замок с ключом

Боб
замок с ключом



Как отправить посылку, чтобы никто третий ее не открыл?

Алиса
замок с ключом

Боб
замок с ключом

Как отправить посылку, чтобы никто третий ее не открыл?

Алиса
замок с ключом

Боб
замок с ключом

Как отправить посылку, чтобы никто третий ее не открыл?

Алиса
замок с ключом

Боб
замок с ключом

Как отправить посылку, чтобы никто третий ее не открыл? Алгоритм Диффи-Хеллмана

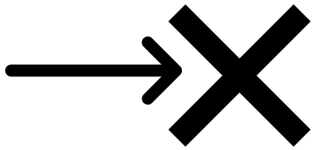
Алиса
замок с ключом

Боб
замок с ключом

MITM

Мэллори

Алиса
замок с ключом

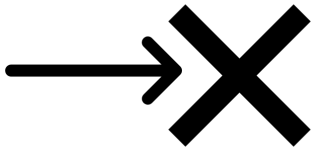


Боб
замок с ключом

MITM

Мэллори

Алиса
замок с ключом

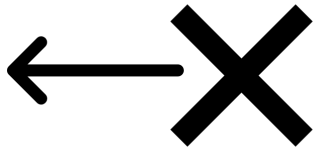


Боб
замок с ключом

MITM

Мэллори

Алиса
замок с ключом



Боб
замок с ключом

MITM

Мэллори

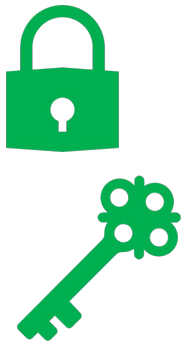
Алиса
замок с ключом

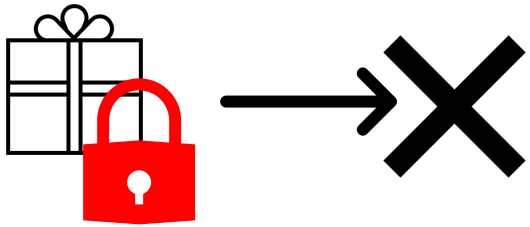
Боб
замок с ключом

MITM

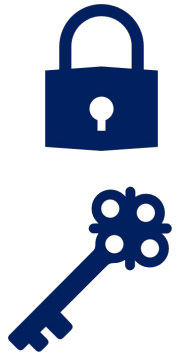
Мэллори

Алиса
замок с ключом



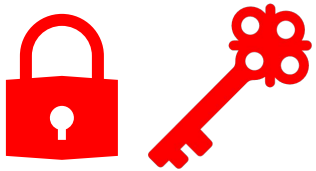


Боб
замок с ключом



MITM

Мэллори



Алиса
замок с ключом

Боб
замок с ключом

Ассиметричное шифрование

Джон

Алиса

Боб

Сара

RSA

Используются в SSL и TLS протоколах.

RSA

1. Возьмем два простых числа p и q.
2. Перемножим их, получим число n — модуль RSA.
3. Рассмотрим магическое число φ = (p – 1) × (q – 1)
4. После этого придумаем e — оно должно быть взаимно простым с φ.
5. Число d — это обратное к e по модулю φ — приватную экспоненту.
6. Пара чисел (n, e) будет открытым ключом, а (n,

RSA

Зашифровываем сообщение m (m < n).
Посчитаем m^e mod n — это будет зашифрованным сообщением.

Считать с помощью Вольфрам Альфа или dcode.fr/en

RSA

$$p = 13, q = 23, n = 299, \varphi = 264$$

$$e = 17, d = 233\ (17 \times 233 = 264 \times 15 + 1)$$

$$m = 25 \rightarrow c = 25^{17}\ mod\ 299 = 64$$

$$c = 64 \rightarrow m = 64^{233}\ mod\ 299 = 25$$