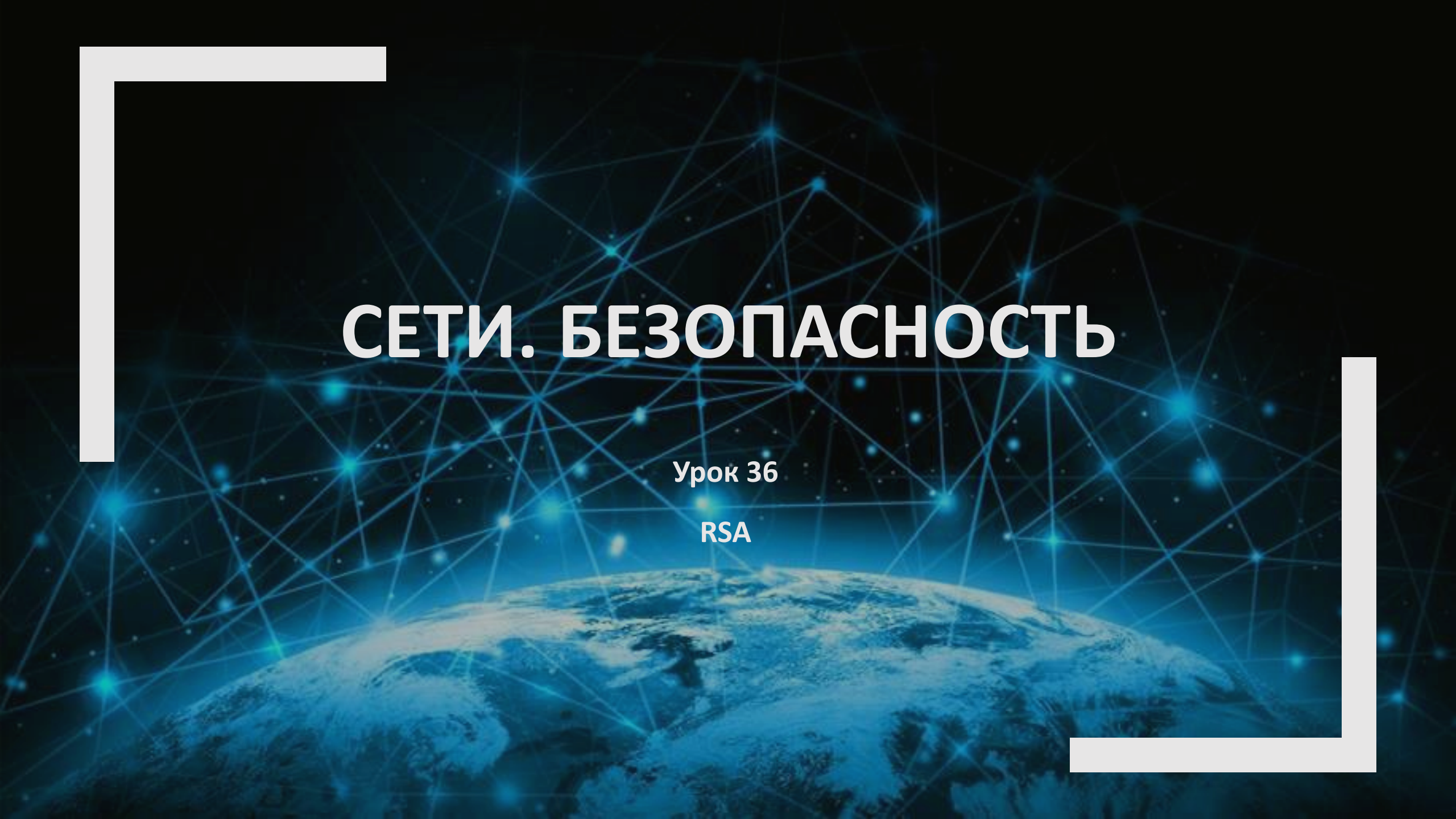


СЕТИ. БЕЗОПАСНОСТЬ

Урок 36

RSA

Публичный ключ

Приватный ключ

d e n

Публичный ключ

e n

Приватный ключ

d n

$M^e \bmod n = Se$

$Se^d \bmod n = M$

Основы алгоритма. Повторяем

1. У каждого участника есть закрытый и открытый ключи
2. Закрытый ключ держится в секрете
3. Открытый ключ можно даже опубликовать в Интернете
4. Открытый и закрытый ключи каждого участника обмена сообщениями в криптосистеме RSA образуют «согласованную пару» в том смысле, что они являются взаимно обратными

Схема RSA

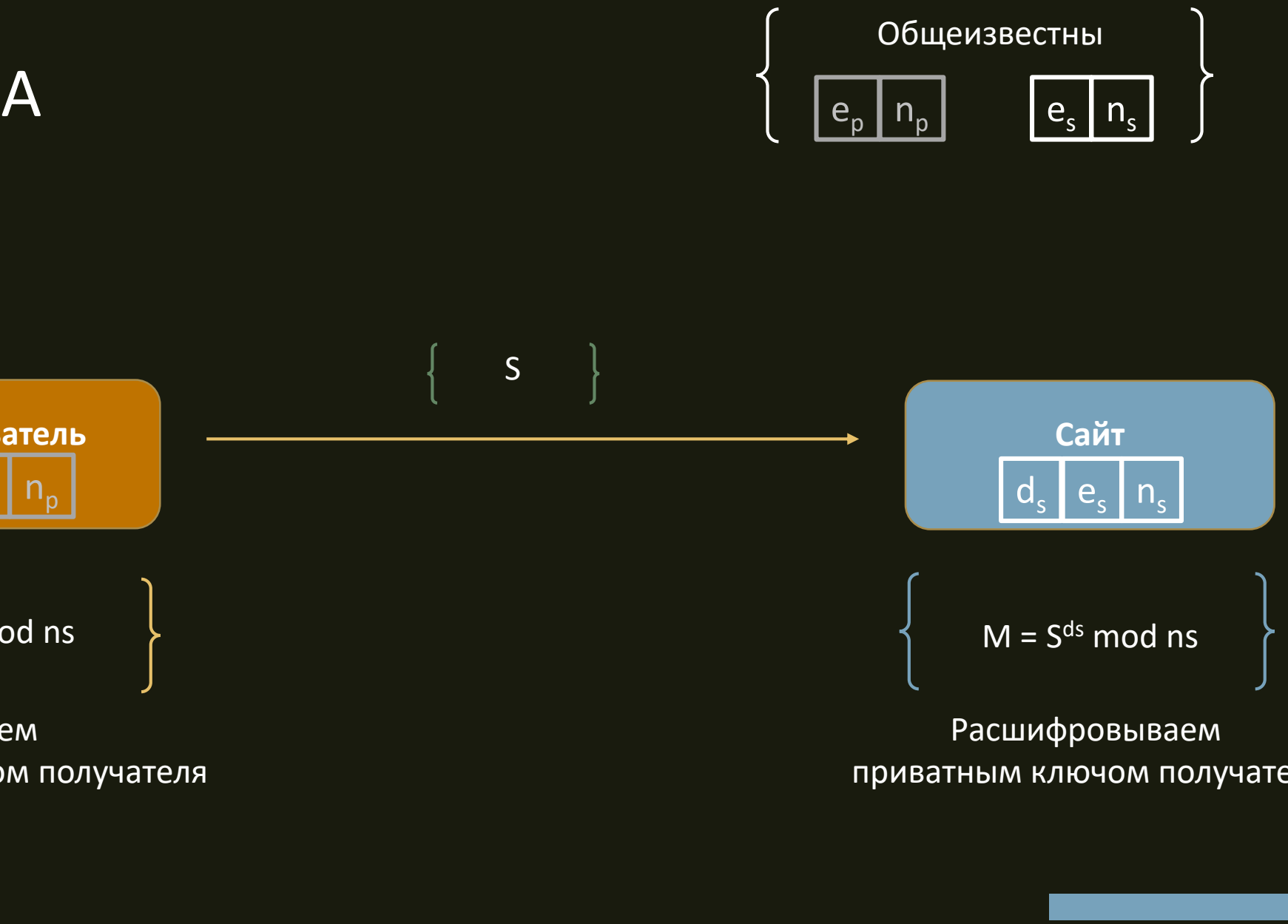
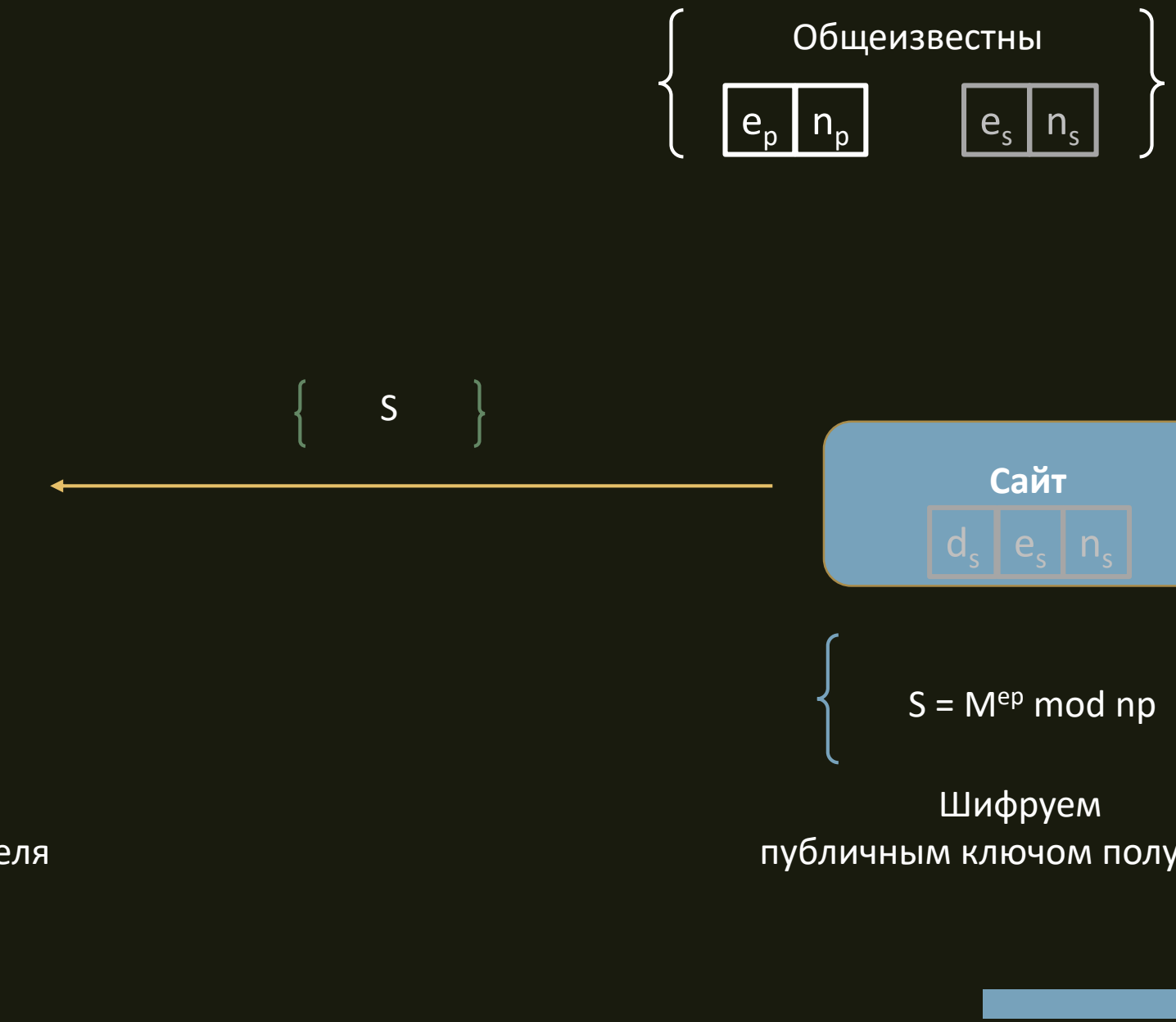
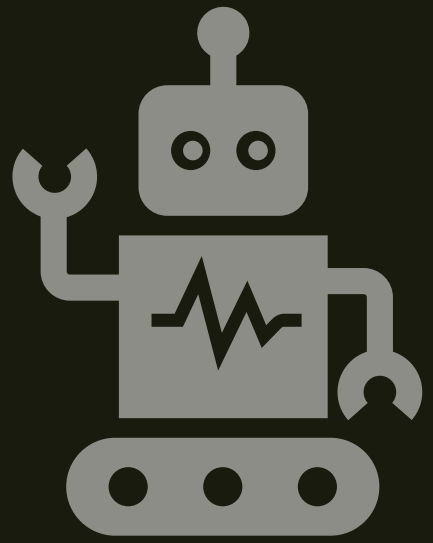

Общеизвестны
e_p n_p
e_s n_s
S
Пользователь
d_p e_p n_p
Сайт
d_s e_s n_s
$S = M^{es} \bmod ns$
$M = S^{ds} \bmod ns$
Шифруем
публичным ключом получателя
Расшифровываем
приватным ключом получателя

Схема RSA


Общеизвестны
e_p n_p
e_s n_s
S
Пользователь
d_p e_p n_p
Сайт
d_s e_s n_s
$M = S^{dp} \bmod np$
$S = M^{ep} \bmod np$
Расшифровываем приватным ключом получателя
Шифруем публичным ключом получателя

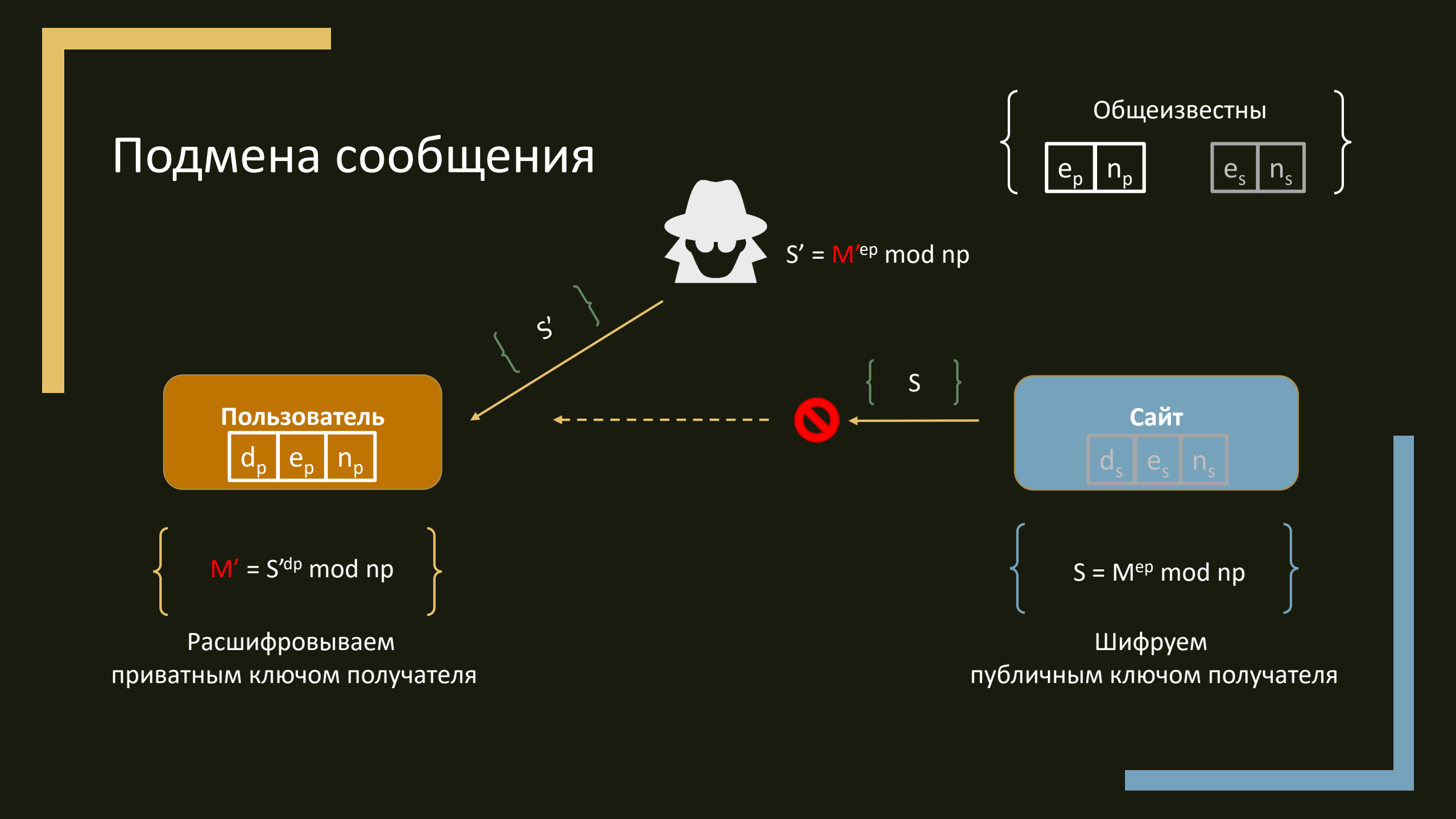
Практика



Аутентификация

Вы получили сообщение. Расшифровали. Получили информацию. Только вот правдивую ли информацию вы получили? Как проверить?

Подмена сообщения



Расшифровываем
приватным ключом получателя

Шифруем
публичным ключом получателя

ЭЦП

- Подтверждение подлинности отправителя
- Подтверждение подлинности документа
- Подтверждает факт отсылки сообщения

- Приравнена законом к личной подписи
- Позволяет реализовать сложные схемы с раздельной доставкой документа и подписи

Как ее передать?

Алгоритм создания подписи

1. Берем открытый текст m
2. Создаем цифровую подпись простой формулой: $s = m^d \bmod n$
3. Передаем пару m и s, чтобы отправить и сообщение, и подпись

Алгоритм проверки подписи

1. Берем пару m и s
2. Берем открытый ключ нашего собеседника
3. Вычисляем сообщение из подписи по формуле: $M = s^e \bmod n$
4. Проверяем подлинность подписи. M и m должны быть равны!

Схема ЭЦП

Общеизвестны

e_p n_p e_s n_s

Пользователь

d_p e_p n_p

E

Сайт

d_s e_s n_s

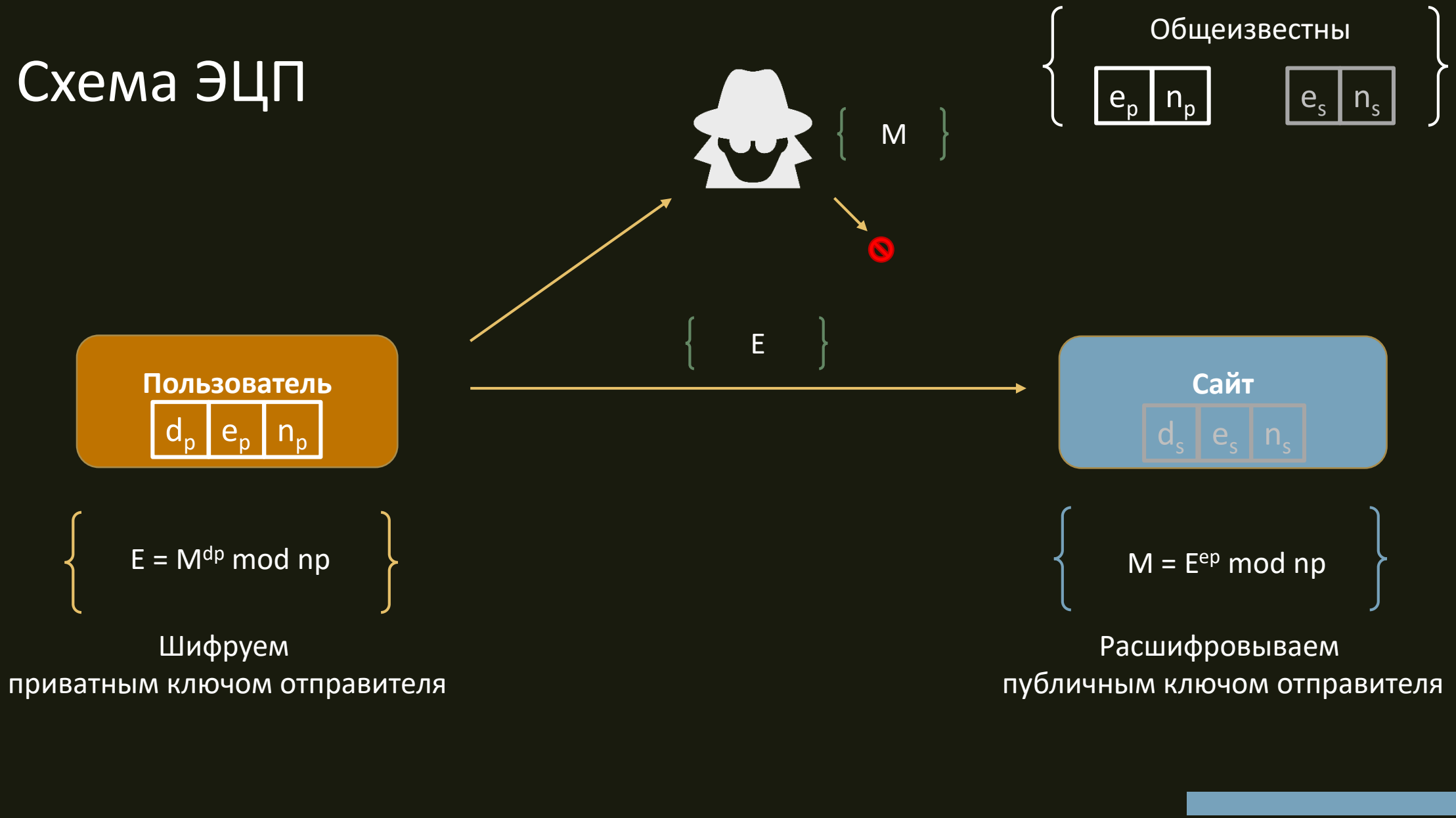
$E = M^{dp} \bmod np$

Шифруем
приватным ключом отправителя

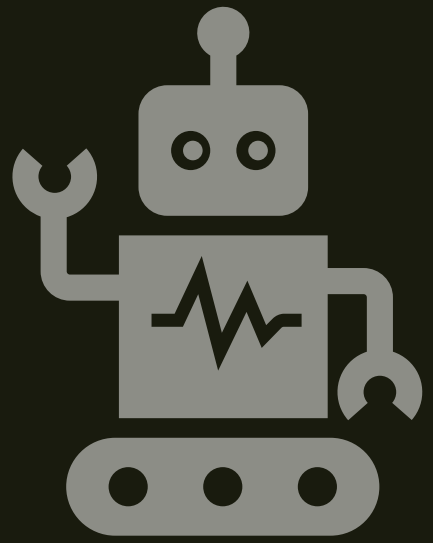
$M = E^{ep} \bmod np$

Расшифровываем
публичным ключом отправителя

Схема ЭЦП


Общеизвестны
e_p n_p
e_s n_s
M
E
Пользователь
d_p e_p n_p
Сайт
d_s e_s n_s
$E = M^{dp} \bmod np$
$M = E^{ep} \bmod np$
Шифруем
приватным ключом отправителя
Расшифровываем
публичным ключом отправителя

Практика



Хеш-сумма

Хеш-сумма – математическая функция от входной строки

Функционал:

- Произвольная длина входных данных
- Фиксированная длина результата
- Однозначность результата

CRC32: F6DE2FEA
MD5: *026f8e459c8f89ef75fa7a78265a0025*
SHA-1: 7DD987F846400079F4B03C058365A4869047B4A0

Качество

- Сильная зависимость результата от входных данных
- Непредсказуемость результата

Стойкость

- Необратимость
- Стойкость к коллизиям первого рода: невозможно подобрать сообщение под известный хеш
- Стойкость к коллизиям второго рода: невозможно подобрать пару сообщений с одинаковым хешом

Хеш-сумма

“Очень длинный текст”

CRC32: 26485bdb
MD5: *c3f0ea667cca19f2b2cbc477392ecdf9*

“Очень длиныый текст”

CRC32: 02bff23e
MD5: *f60f8f645ebe88f22515e44c534153a0*

Схема ЭЦП

Общеизвестны

e_p n_p e_s n_s

Пользователь

d_p e_p n_p

M, E

Сайт

d_s e_s n_s

hm=Hash(M)

$E = hm^{dp} \bmod np$

Шифруем
приватным ключом отправителя

hm=Hash(M)

$hm' = E^{ep} \bmod np$

hm==hm’

Расшифровываем
публичным ключом отправителя

Бонус

Слепая ЭЦП

Общеизвестны

e_p n_p e_s n_s

Пользователь

d_p e_p n_p

S1, S2, E

Сайт

d_s e_s n_s

$M = m1,m2$

$S1 = m1^{es} \bmod ns$

$S2 = m2^{ep} \bmod np$

$hm = Hash(S1,S2)$

$E = hm^{dp} \bmod np$

Слепая ЭЦП

Общеизвестны

e_p n_p e_s n_s

Пользователь

d_p e_p n_p

Сайт

d_s e_s n_s

S1, S2, E

$M = m1,m2$

$S1 = m1^{es} \bmod ns$

$S2 = m2^{ep} \bmod np$

$hm=Hash(S1,S2)$

$E = hm^{dp} \bmod np$

…ES1, ES2, …

$Hm = Hash(S1,S2)$

$hm' = E^{ep} \bmod np$

$hm==hm'$

$m1 = S1^{ds} \bmod ns$

$ES1 = m1^{ds} \bmod ns$

$ES2 = S2^{ds} \bmod ns$

…

Слепая ЭЦП

Общеизвестны: e_p n_p e_s n_s

Пользователь: d_p e_p n_p

Сайт: d_s e_s n_s

S1, S2, E →

M = m1,m2
$S1 = m1^{es} \bmod ns$
$S2 = m2^{ep} \bmod np$

hm=Hash(S1,S2)
$E = hm^{dp} \bmod np$

← …ES1, ES2, …

Hm = Hash(S1,S2)
$hm' = E^{ep} \bmod np$
hm==hm’
$m1 = S1^{ds} \bmod ns$

$ES1 = m1^{ds} \bmod ns$
$ES2 = S2^{ds} \bmod ns$
…

…

$ES2^{dp} \bmod np = (S2^{ds} \bmod ns)^{dp} \bmod np =$
$=[(m2^{ep} \bmod np)^{ds} \bmod ns]^{dp} \bmod np =$
$=[(m2^{ep} \bmod np)^{dp} \bmod np]^{ds} \bmod ns =$
$=m2^{ds} \bmod ns$

Практика