СЕТИ. БЕЗОПАСНОСТЬ

Урок 37

RSA, сертификаты и мандаты

Вспоминаем RSA

1. У каждого участника есть закрытый ключ d, открытый ключ e и модуль n
2. Закрытый ключ держится в секрете, открытый публикуется для всех участников
3. Шифровка: $C = M^e \bmod n$, где C – зашифрованное сообщение
4. Расшифровка: $M = C^d \bmod n$, где M – расшифрованное сообщение

d e n

Публичный ключ

e n

Приватный ключ

d n

$M^e \bmod n = Se$

$Se^d \bmod n = M$

Схема RSA

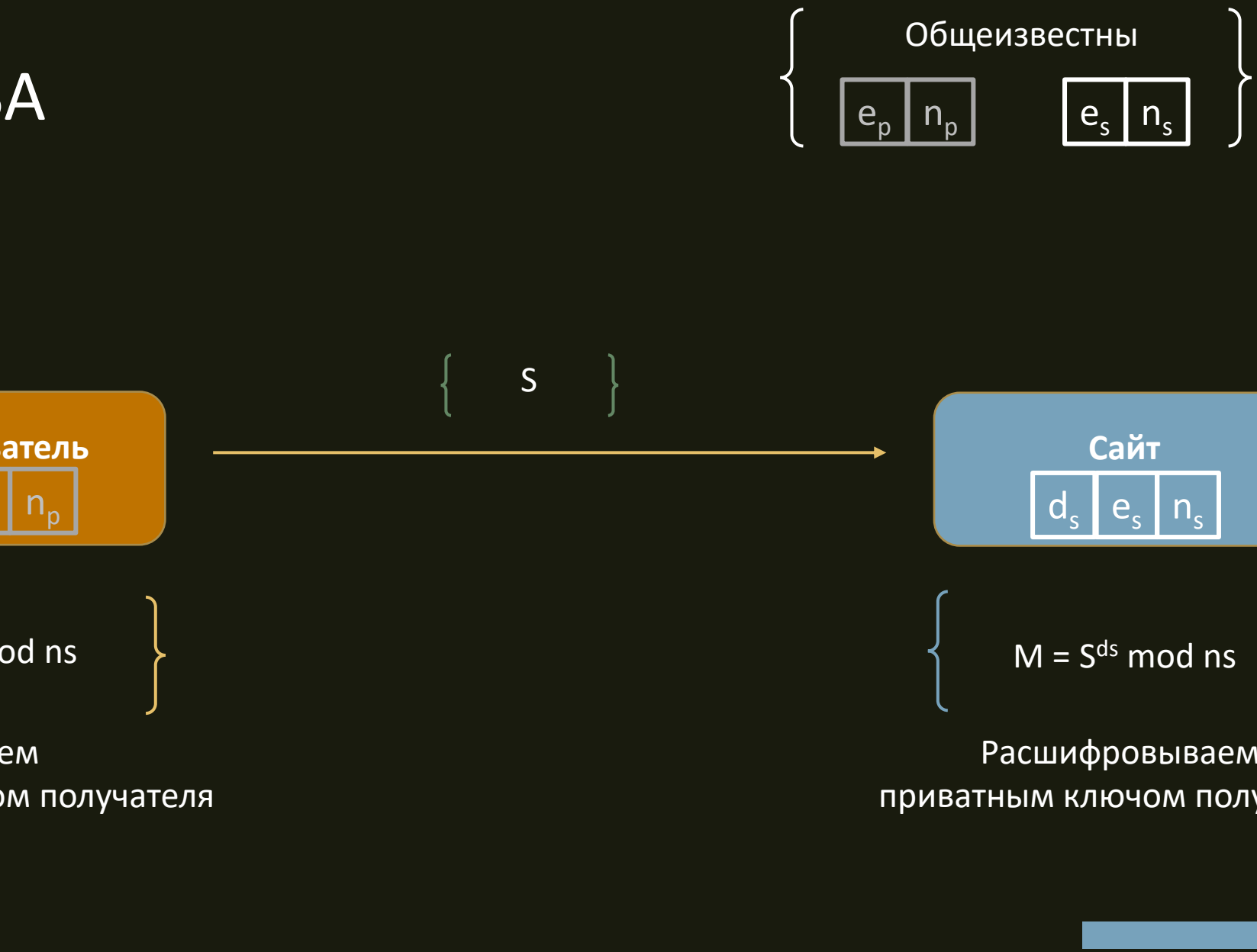

Общеизвестны
e_p n_p
e_s n_s
S
Пользователь
d_p e_p n_p
Сайт
d_s e_s n_s
$S = M^{es} \bmod ns$
$M = S^{ds} \bmod ns$
Шифруем
публичным ключом получателя
Расшифровываем
приватным ключом получателя

Схема 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

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

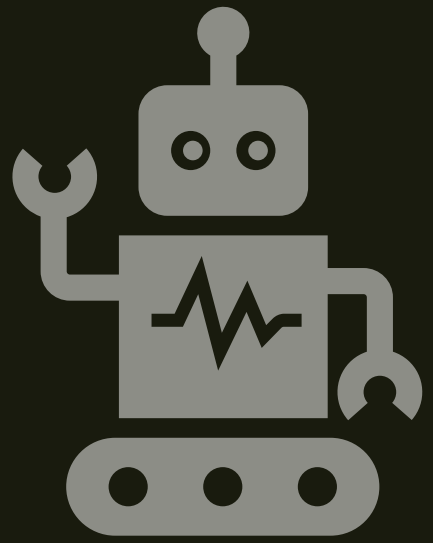
hm=Hash(M)

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

hm==hm’

Расшифровываем
публичным ключом отправителя

Практика



Подмена

Общеизвестны

e_p n_p — Пользователь

e_s n_s

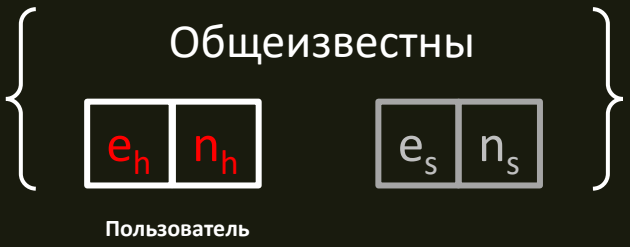
Пользователь

d_p e_p n_p

Сайт

d_s e_s n_s

Подмена



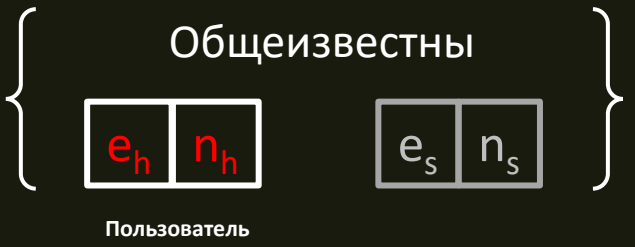
Пользователь

d_p e_p n_p

Сайт

d_s e_s n_s

Подмена



M, E

Пользователь

d_p e_p n_p

O_o
????

Сайт

d_s e_s n_s

hm=Hash(M)
hm'= E^{ep} mod np
hm==hm’

Расшифровываем
публичным ключом отправителя

Сертификаты

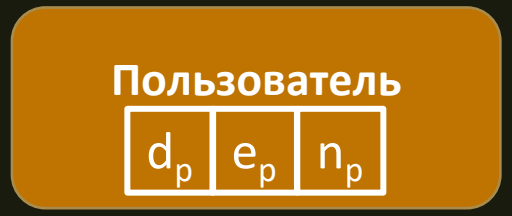
Пользователь

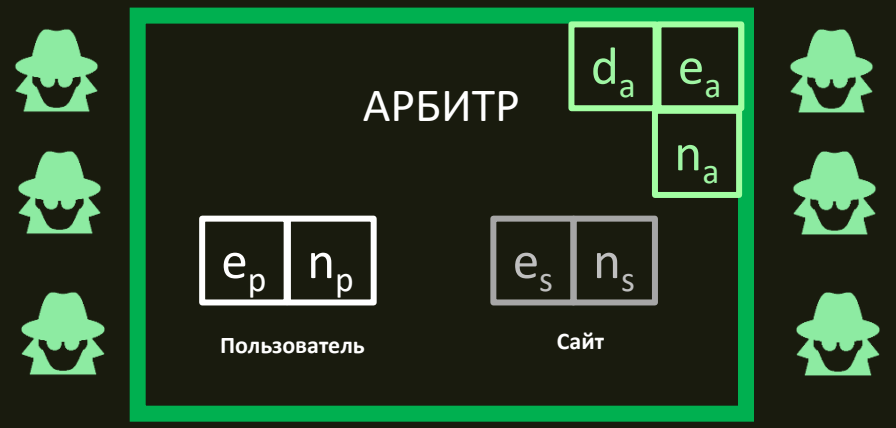
d_p	e_p	n_p

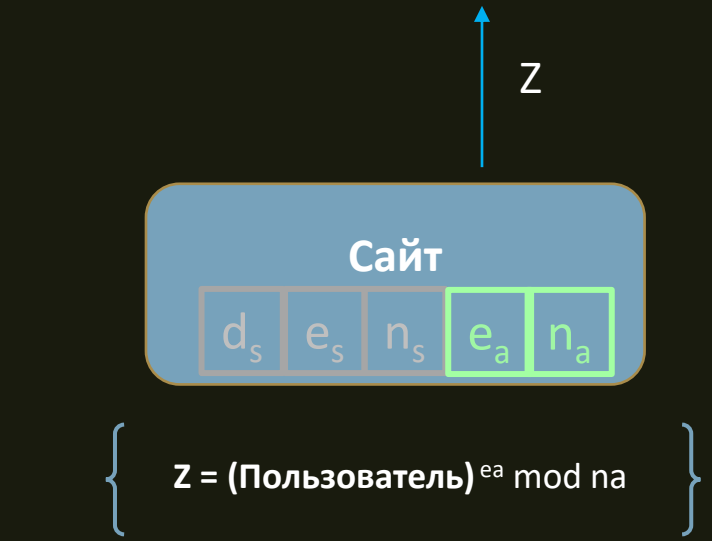
Сайт

d_s	e_s	n_s	e_a	n_a

Сертификаты

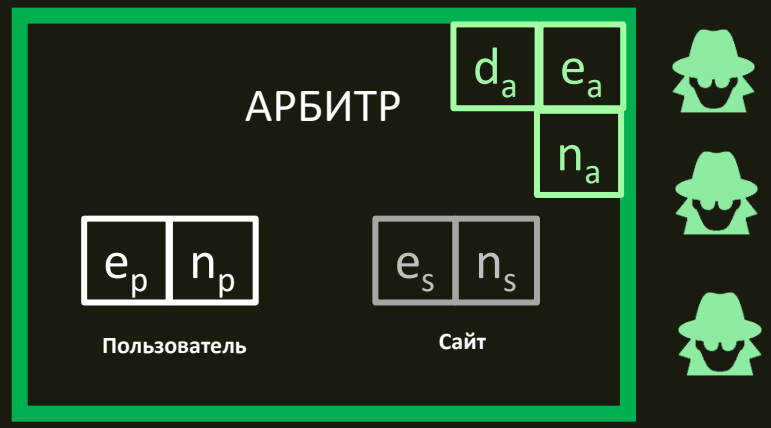


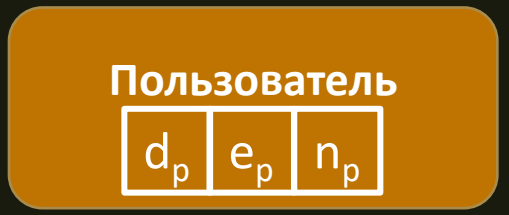


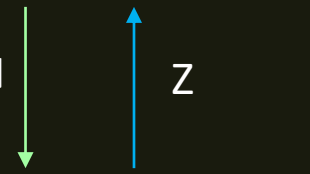


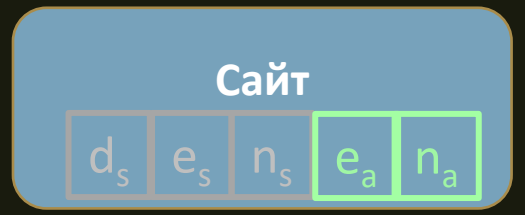
Сертификаты

$$\begin{cases} ZE = [e_p]^{da} \bmod n_a \\ ZN = [n_p]^{da} \bmod n_a \end{cases}$$





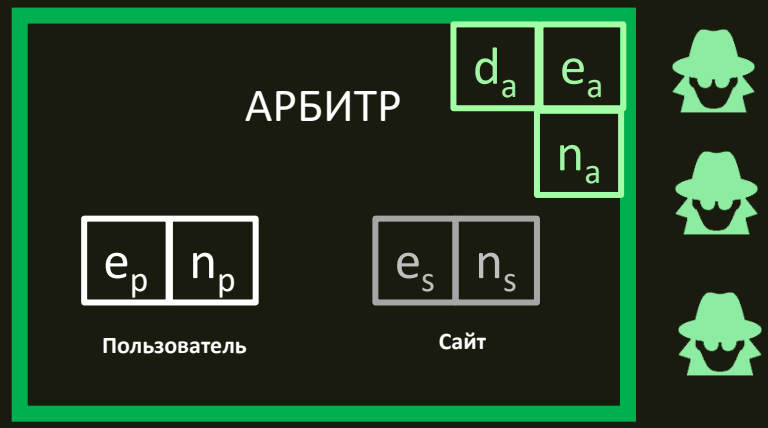




$$\{ \mathbf{Z = (Пользователь)}^{ea} \bmod na \}$$

Сертификаты

$$\begin{cases} ZE = [e_p]^{da} \bmod n_a \\ ZN = [n_p]^{da} \bmod n_a \end{cases}$$



ZE, ZN

Z

Пользователь

d_p e_p n_p

Сайт

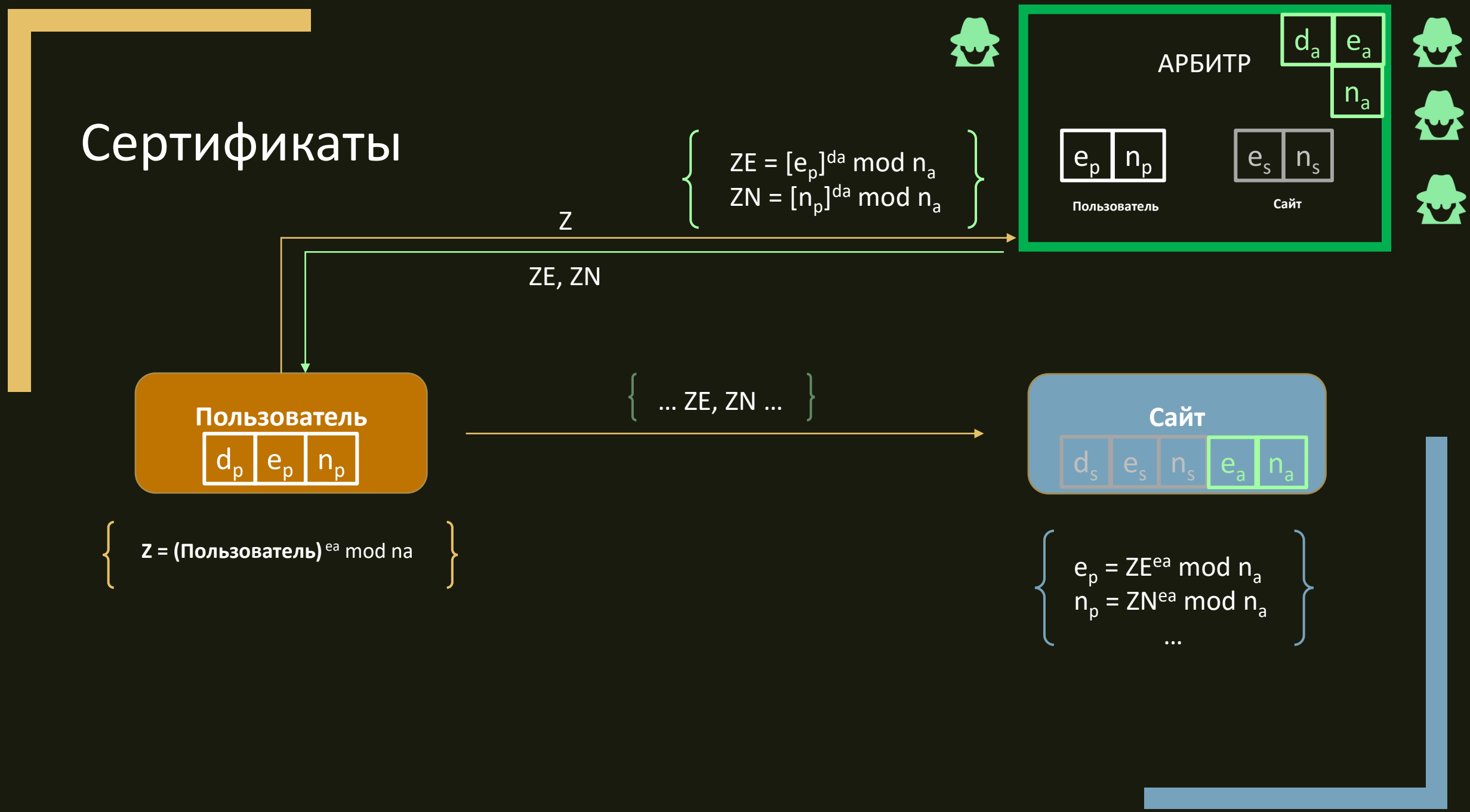
d_s e_s n_s e_a n_a

$$\begin{cases} \mathbf{Z = (Пользователь)}^{ea} \bmod na \end{cases}$$

$$\begin{cases} e_p = ZE^{ea} \bmod n_a \\ n_p = ZN^{ea} \bmod n_a \end{cases}$$

RSA, ЭЦП…

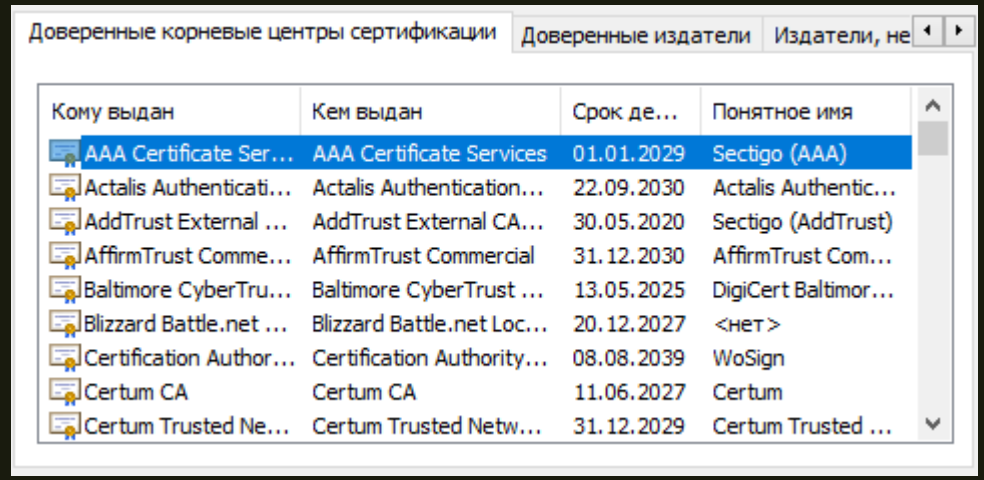
Сертификаты



Сертификаты

- Подтверждает подлинность ключей
- Подтверждает подлинность собеседника/сайта
- Требует наличия доверенного арбитра

- Бывают самоподписанными



Практика

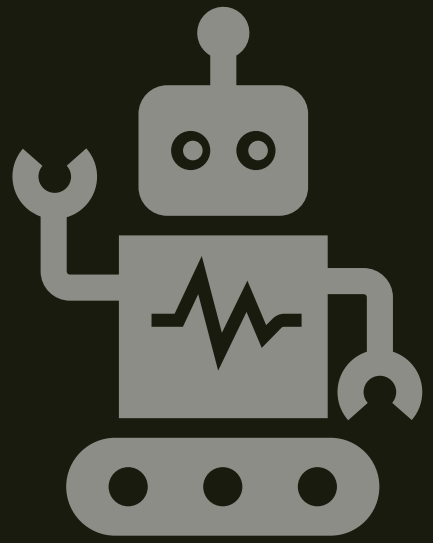


Схема мандата

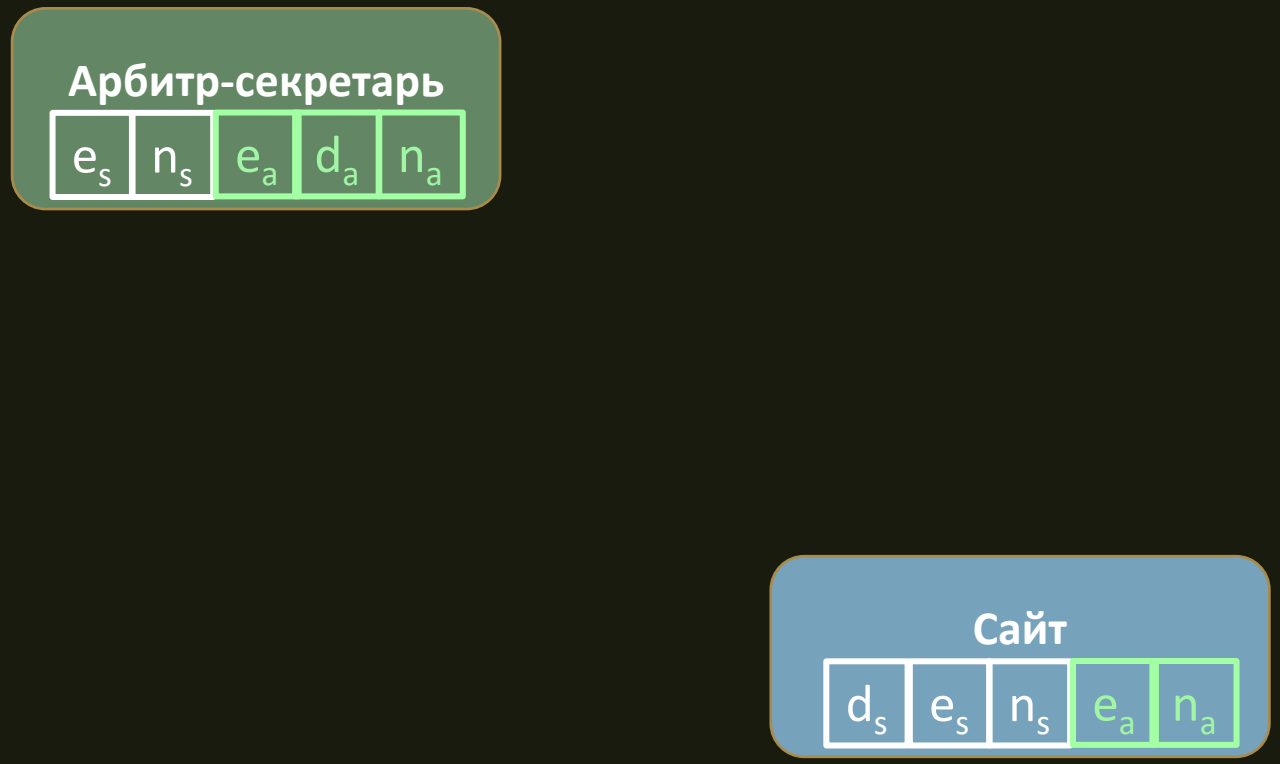


Схема мандата

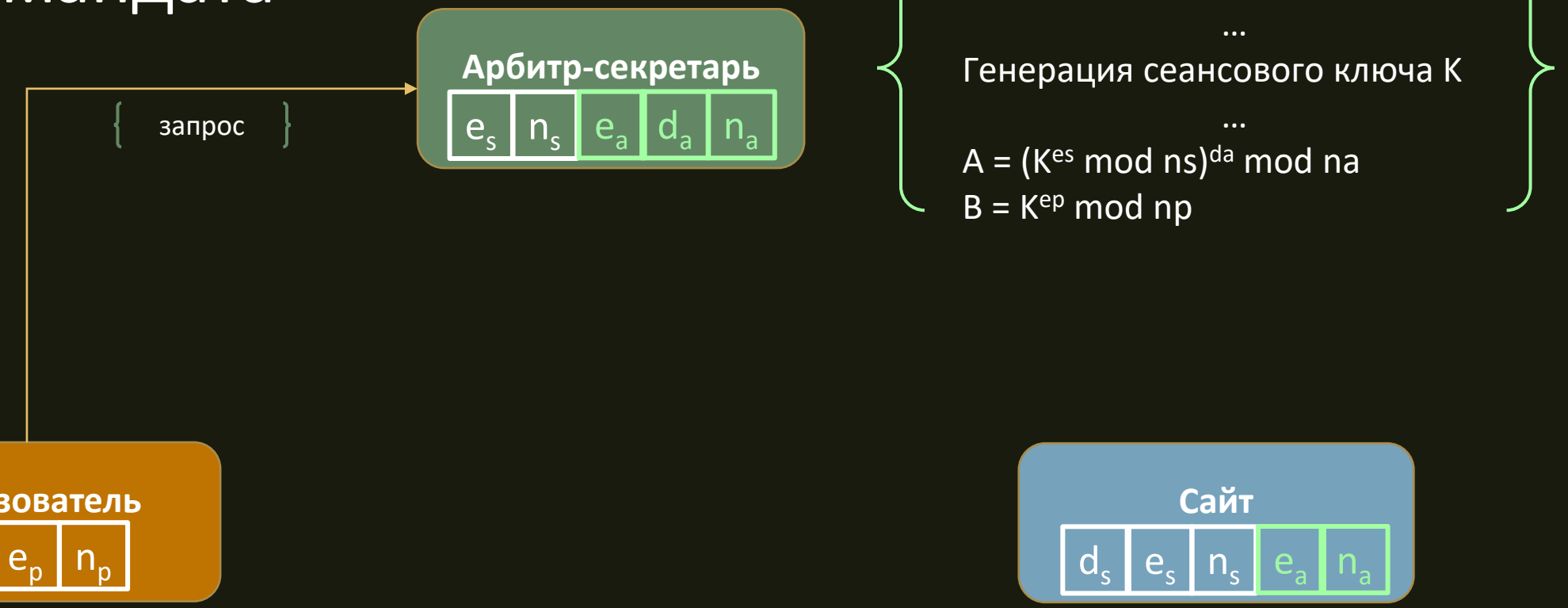
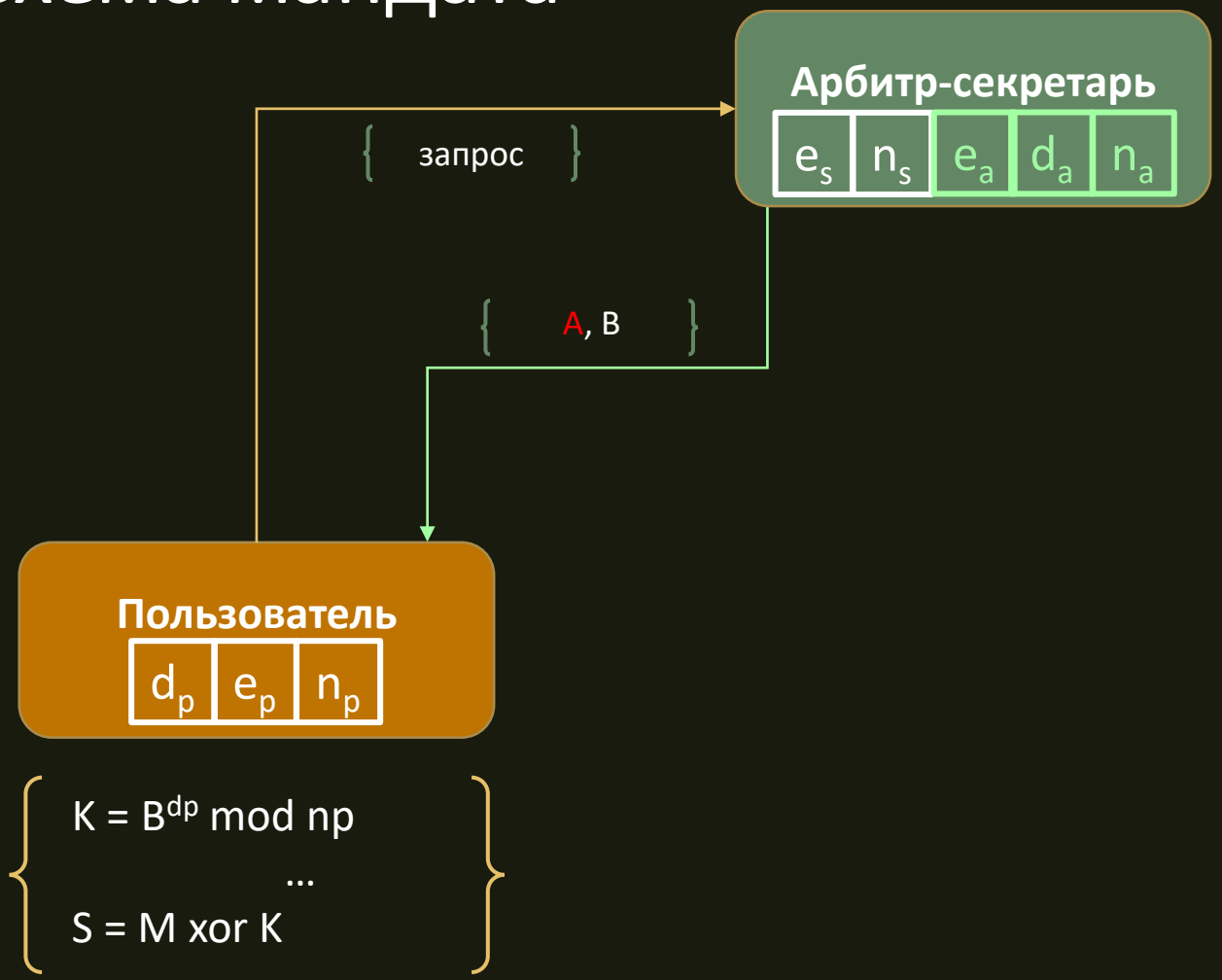


Схема мандата

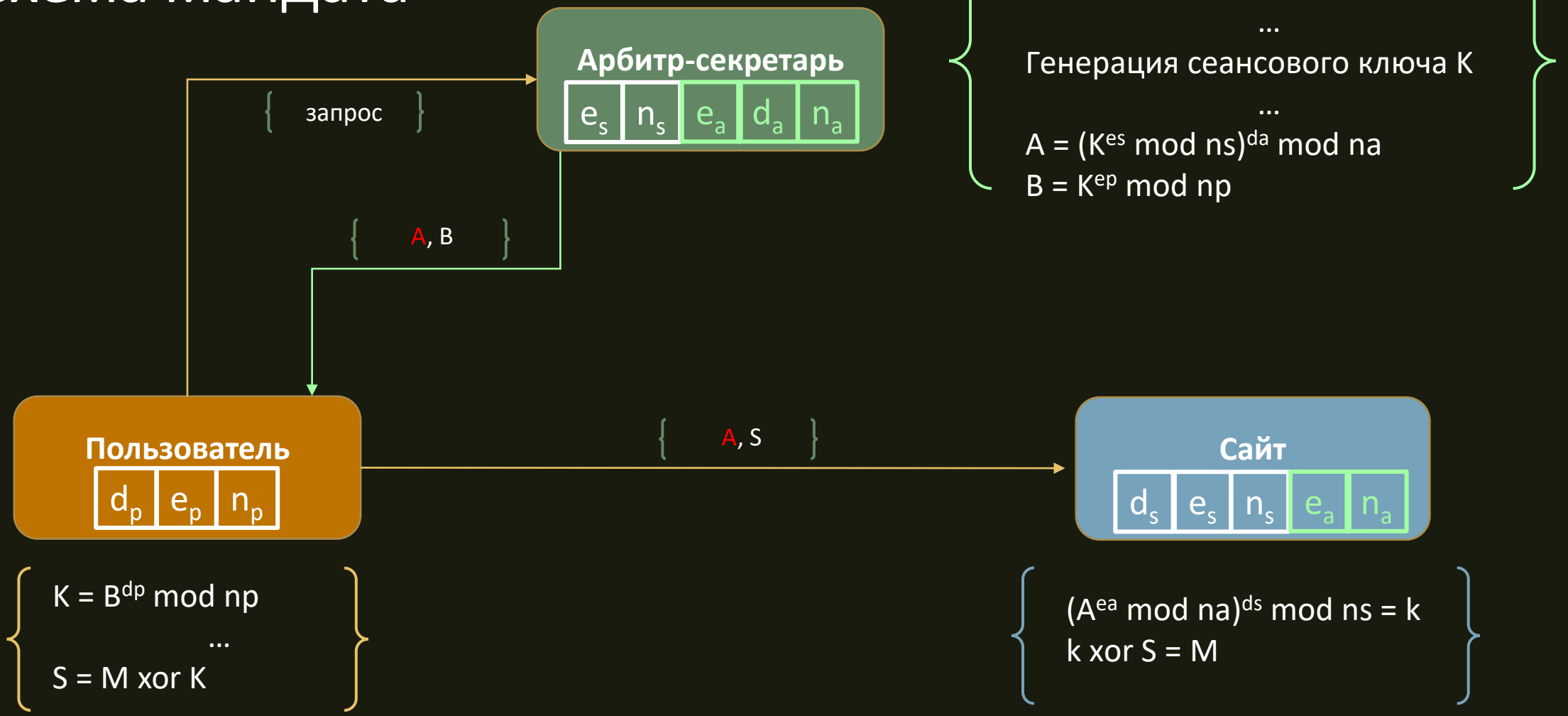


Проверка сертификата
Проверка права и лимита
…
Генерация сеансового ключа K
…
$A = (K^{es} \bmod ns)^{da} \bmod na$
$B = K^{ep} \bmod np$

Сайт

d_s e_s n_s e_a n_a

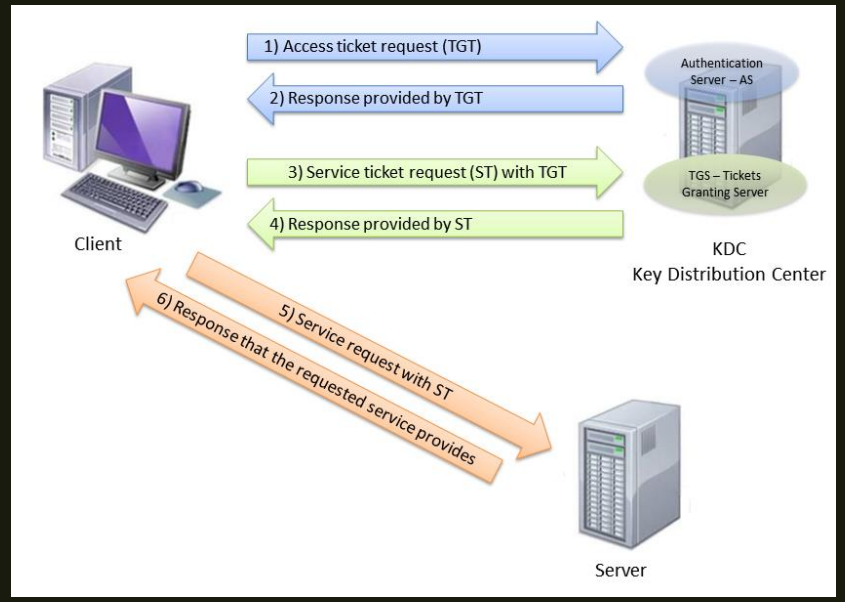
Схема мандата



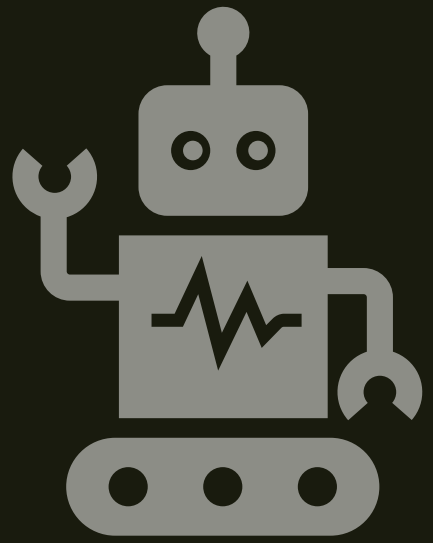
Мандаты

1. Подлинность отправителя
2. Подлинность получателя
3. Право и очередь отправителя на общение с получателем

4. Экономия времени и ресурсов основного сервера



Практика



Рецепты

1. RSA открывается секретным ключом получателя
2. RSA закрывается публичным ключом получателя

3. ЭЦП открывается публичным ключом отправителя
4. ЭЦП ставится секретным ключом отправителя

5. Сертификат содержит публичный ключ третьего лица. Вскрывается публичным ключом арбитра.
6. Самоподписанный сертификат тождественен ЭЦП

7. Мандат для отправителя: второе число вскрывается своим секретным ключом
8. Мандат для получателя: вскрывать сначала публичным ключом арбитра, затем секретным своим

Общая схема

1. Подготовка сообщения и сеансового ключа шифрования
2. Запрос сертификата Получателя у Арбитра
3. Передача по RSA сеансового ключа K
4. Хеширование сообщения отправителем
5. Подпись Хеша
6. Шифрование сообщения и подписи
7. Передача сообщения и подписи
8. Запрос сертификата Отправителя у Арбитра
9. Открытие по RSA сеансового ключа K
10. Расшифрование сообщения и подписи
11. Хеширование сообщения
12. Верификация подписи
13. …готово…

Отправка

Получение

Конкурс на лучший рисунок