

СЕТИ. КРИПТОГРАФИЯ

Урок 35

Асимметричное шифрование

Симметричное и асимметричное шифрования

Симметричное

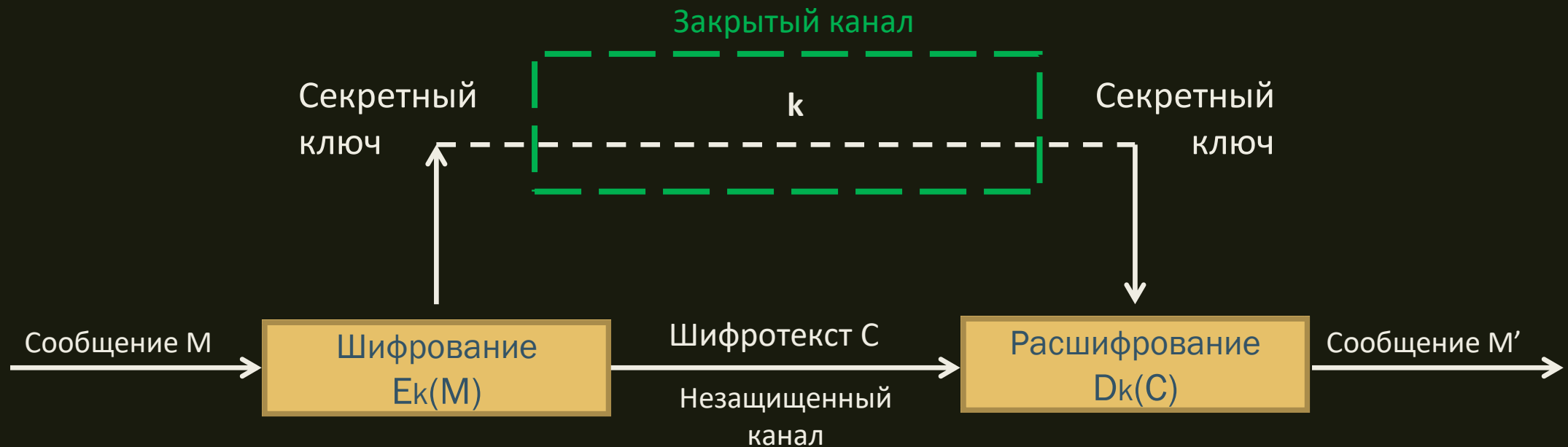
- Простое
- Быстрое
- Эффективное

Асимметричное

- Архисложное
- Долгое
- Мистическое

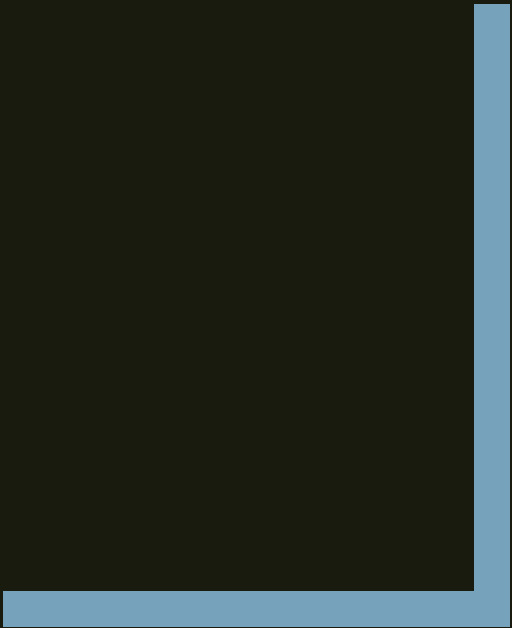
Симметричное шифрование

Решает проблему передачи при наличии закрытого канала

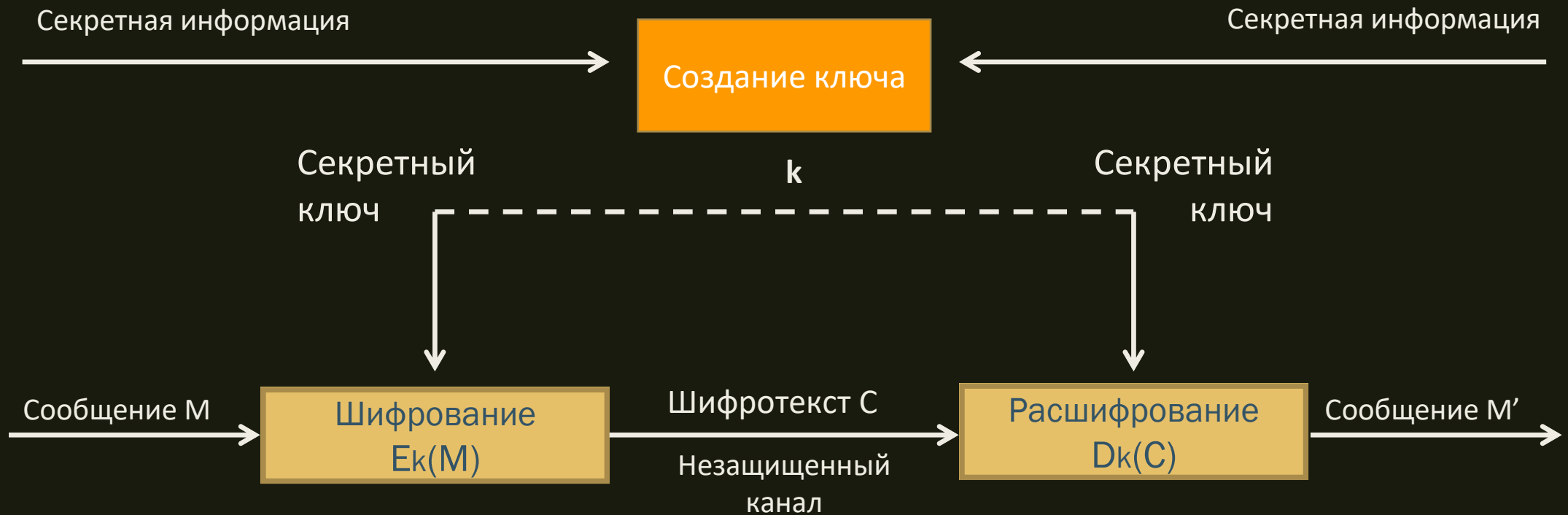




Проблематика

- Нет закрытого канала
 - Подмена сообщения
 - Подмена пользователя
- 

Создание общего секрета



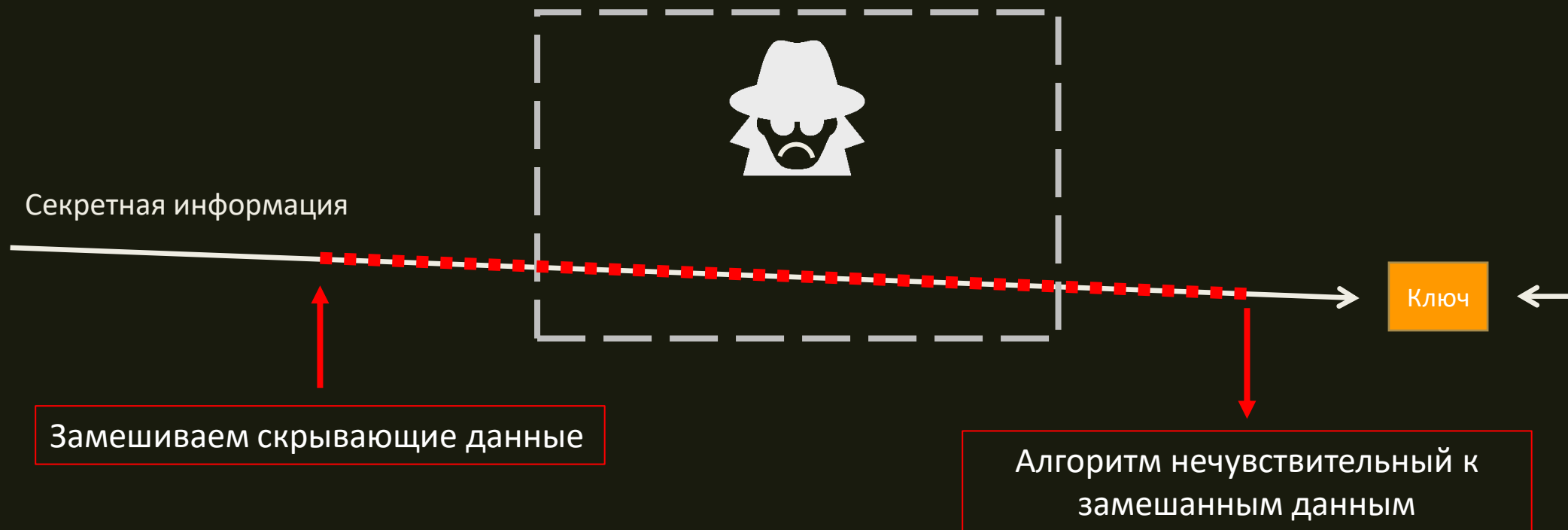
Создание общего секрета



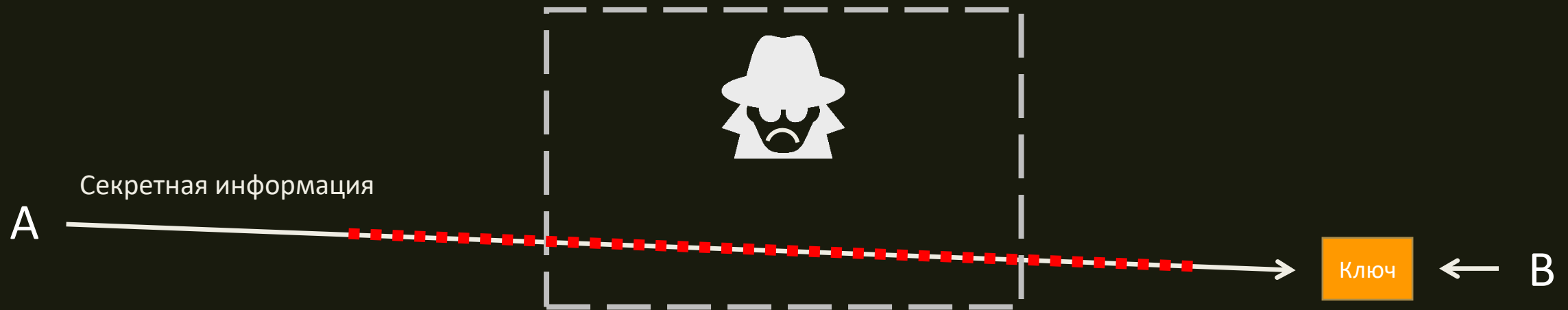
Создание общего секрета



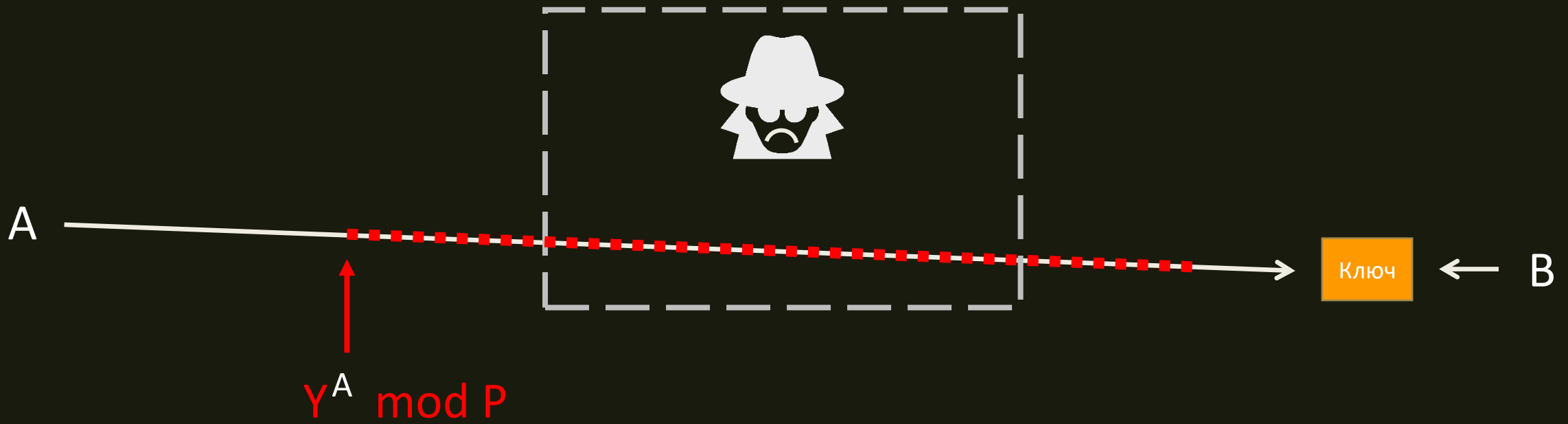
Защита информации



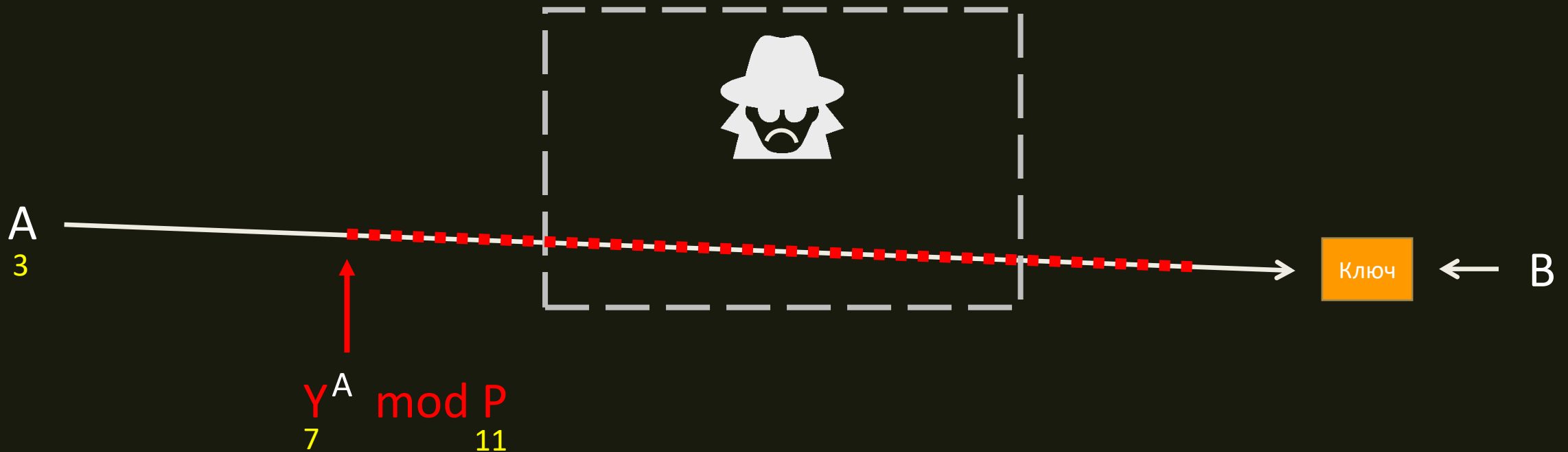
Защита информации



Односторонние функции

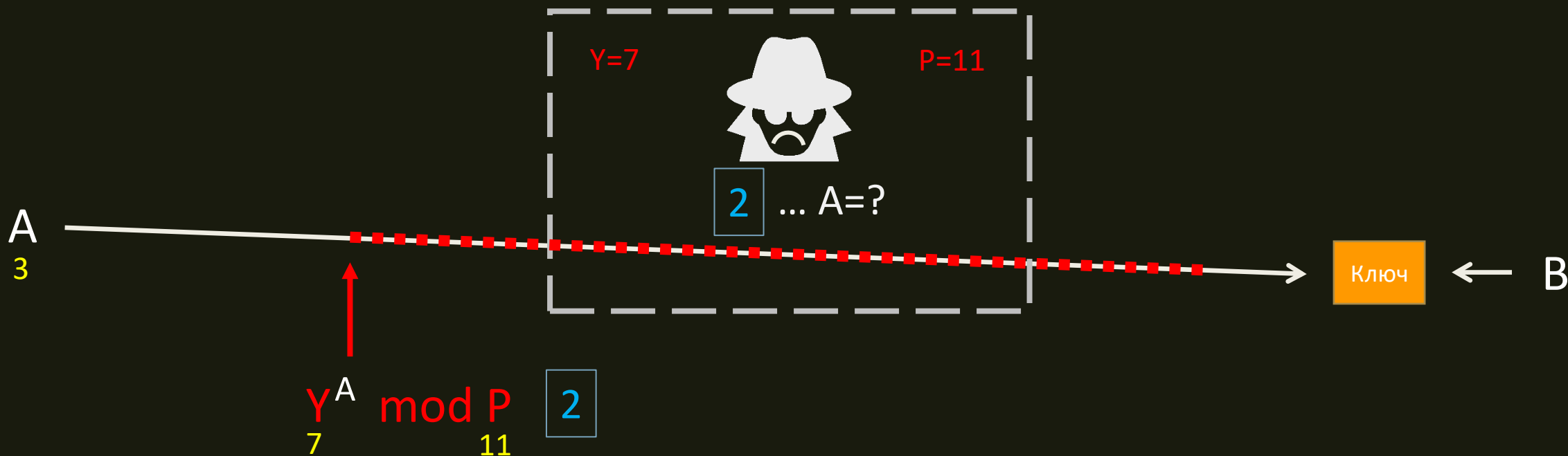


Односторонние функции



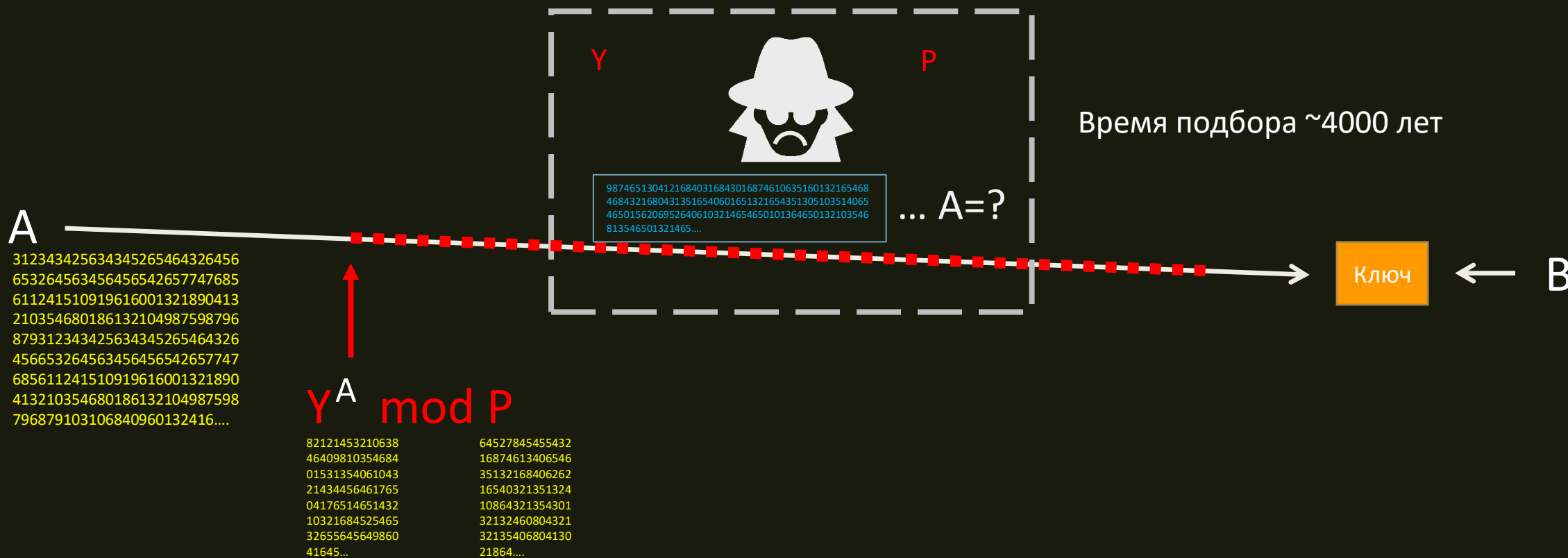
$$7^3 \bmod 11 = 343 \bmod 11 = 2$$

Односторонние функции

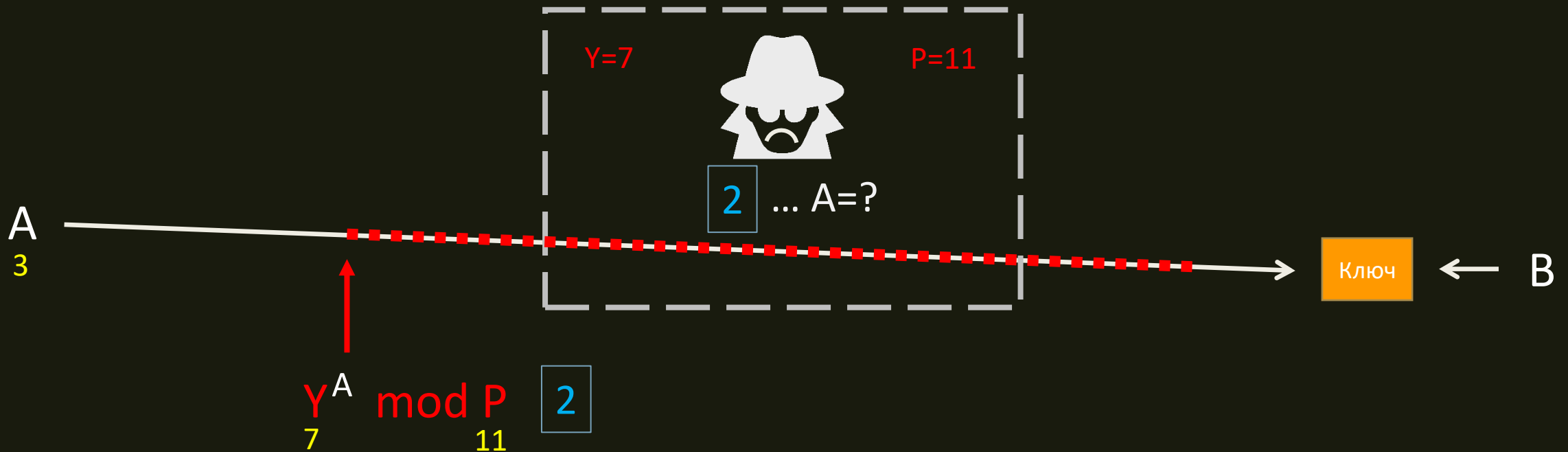


$$7^3 \bmod 11 = 343 \bmod 11 = 2$$

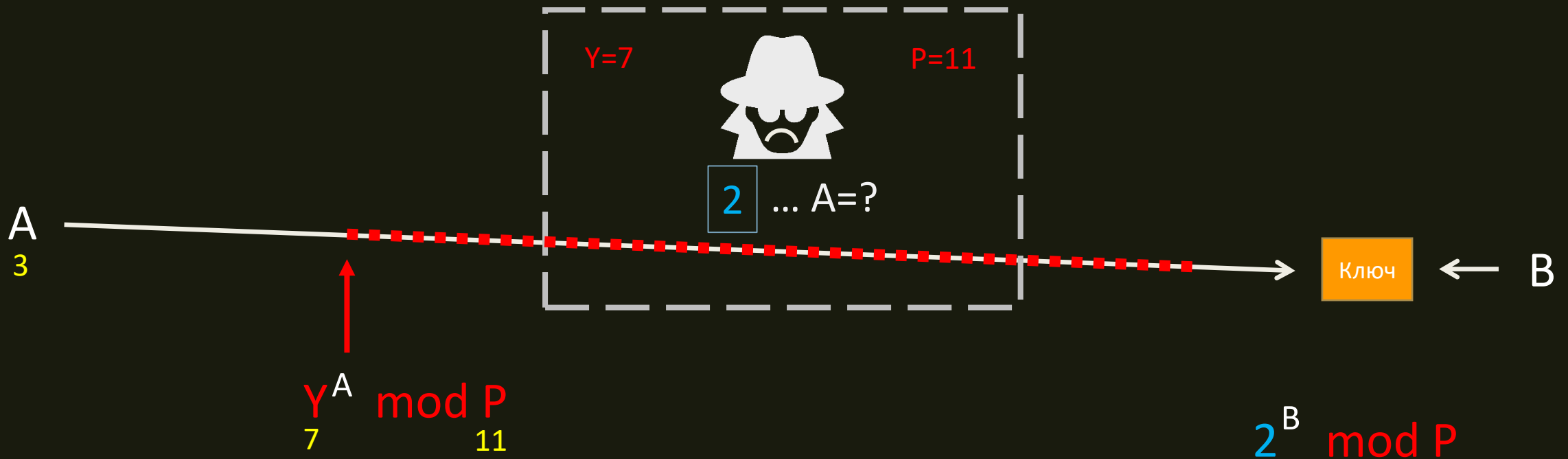
Проблема дискретного логарифмирования



Односторонние функции



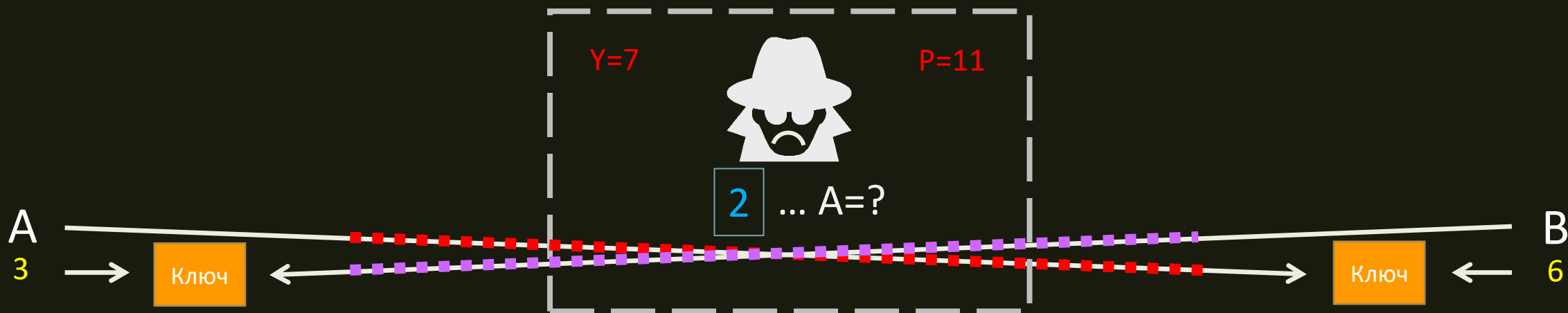
Односторонние функции



Односторонние функции



Односторонние функции

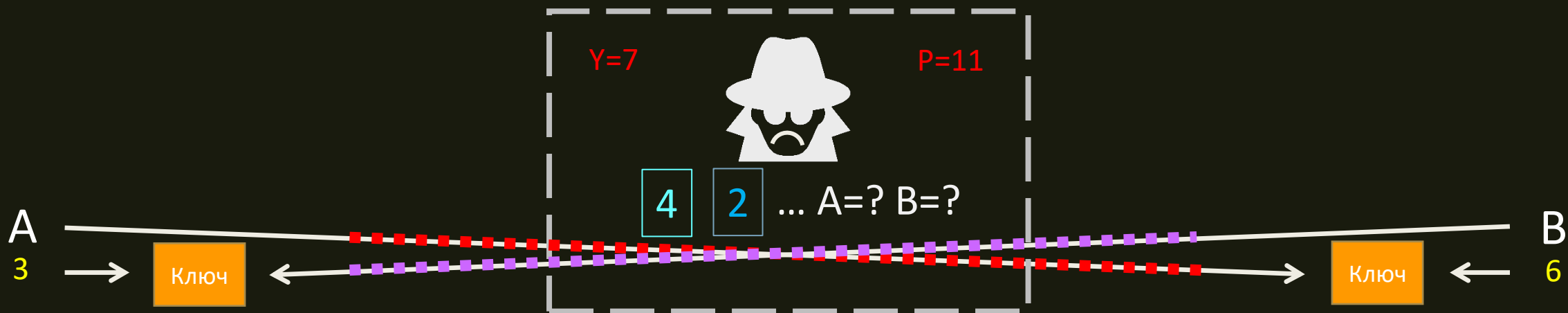


$?^A \bmod P$

$Y^B \bmod P$?

9

Односторонние функции



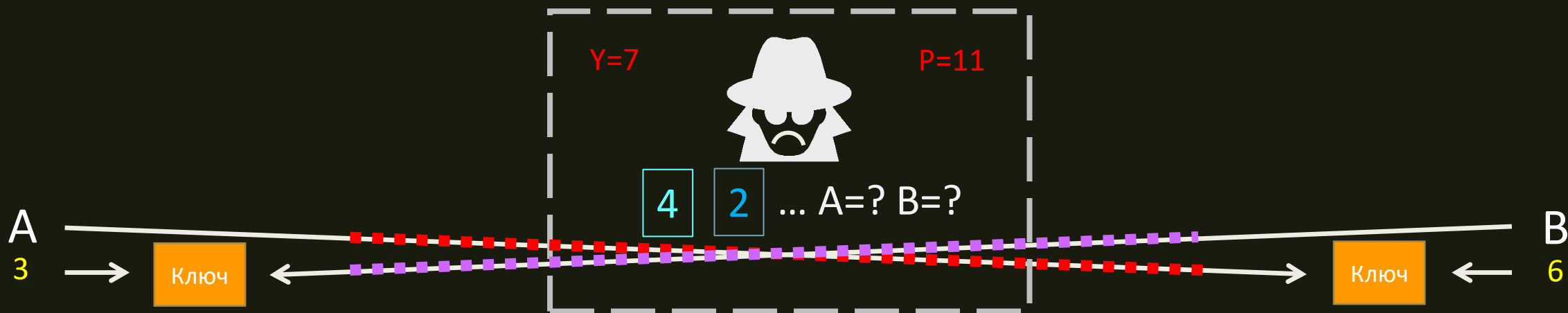
$$4^A \bmod P$$

$$Y^B \bmod P \quad 4$$

$$7^6 \bmod 11 = 117649 \bmod 11 = 4$$

9

Алгоритм Диффи-Хеллмана



$$4^A \bmod P$$

$$4^3 \bmod 11 = 64 \bmod 11 = 9$$

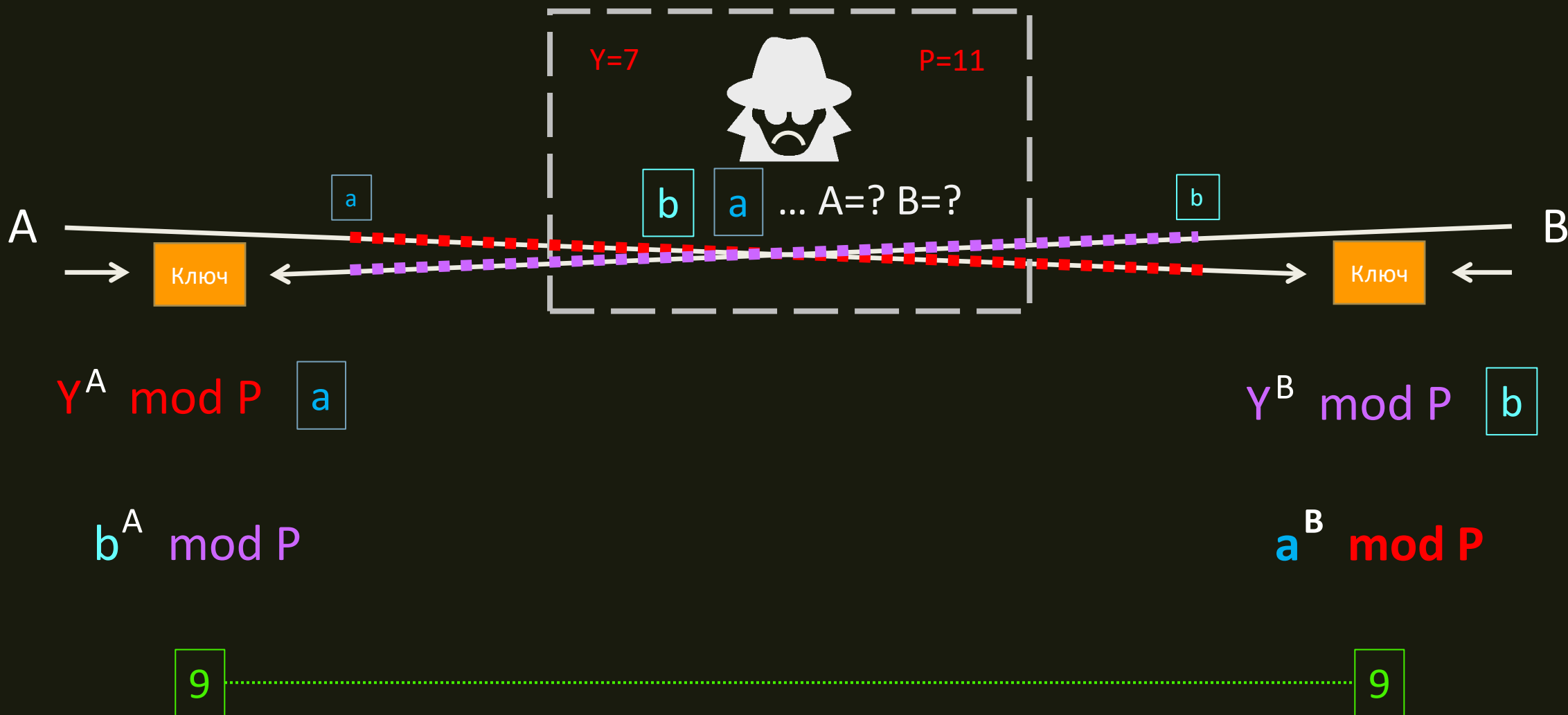
$$Y^B \bmod P$$

4

9

9

Алгоритм Диффи-Хеллмана



Алгоритм Диффи-Хеллмана

$$Y^A \bmod P \quad \boxed{a}$$

$$b^A \bmod P$$

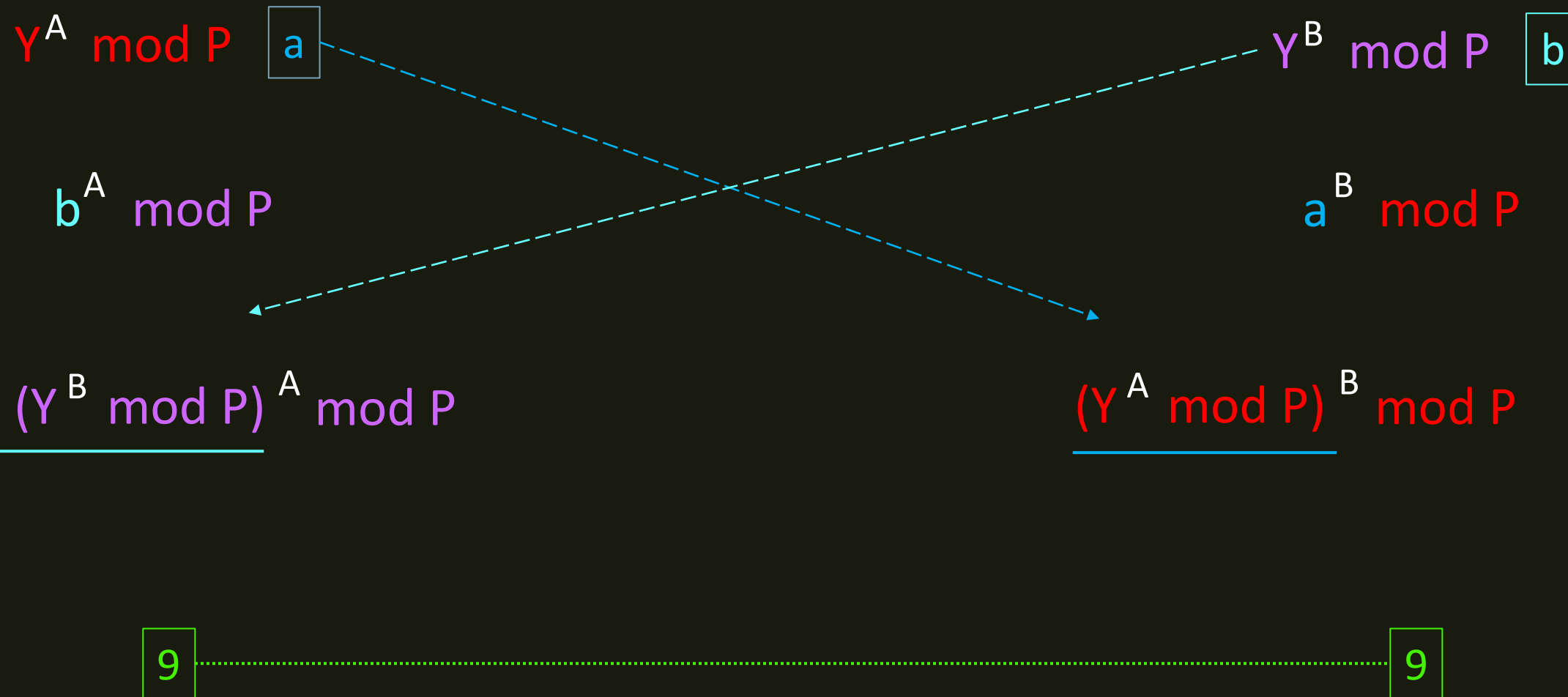
$$Y^B \bmod P \quad \boxed{b}$$

$$a^B \bmod P$$

9

9

Алгоритм Диффи-Хеллмана



Алгоритм Диффи-Хеллмана

$$Y^A \bmod P \quad \boxed{a}$$

$$Y^B \bmod P \quad \boxed{b}$$

$$b^A \bmod P$$

$$a^B \bmod P$$

$$\underline{(Y^B \bmod P)^A \bmod P}$$

$$\underline{(Y^A \bmod P)^B \bmod P}$$

$$Y^{AB} \bmod P$$

9

9

Алгоритм Диффи-Хеллмана

$$\underline{(NM) \bmod P}$$

$$N = a_1 + b_1 P : b_1 = N \bmod P, a_1 = P \cdot r_1$$

$$M = a_2 + b_2 P : b_2 = M \bmod P, a_2 = P \cdot r_2$$

$$((a_1 + b_1 P)(a_2 + b_2 P)) \bmod P$$

$$\underbrace{(a_1 a_2 + a_1 b_2 P + b_1 a_2 P + b_1 b_2 P^2)}_{\text{кратно } P} \bmod P = \underline{b_1 b_2 \bmod P = (N \bmod P)(M \bmod P) \bmod P}$$

$$\underline{(Y^B \bmod P)^A \bmod P}$$

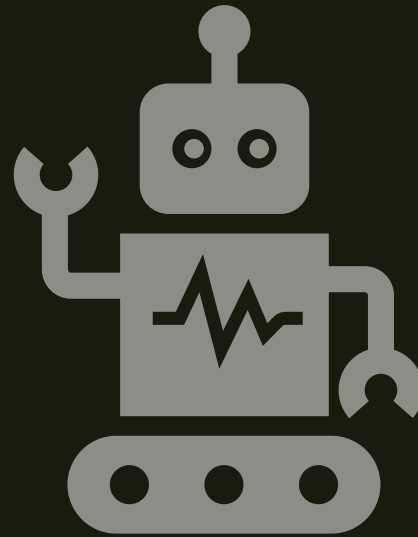
$$\underline{(Y^A \bmod P)^B \bmod P}$$

$$Y^{AB} \bmod P$$

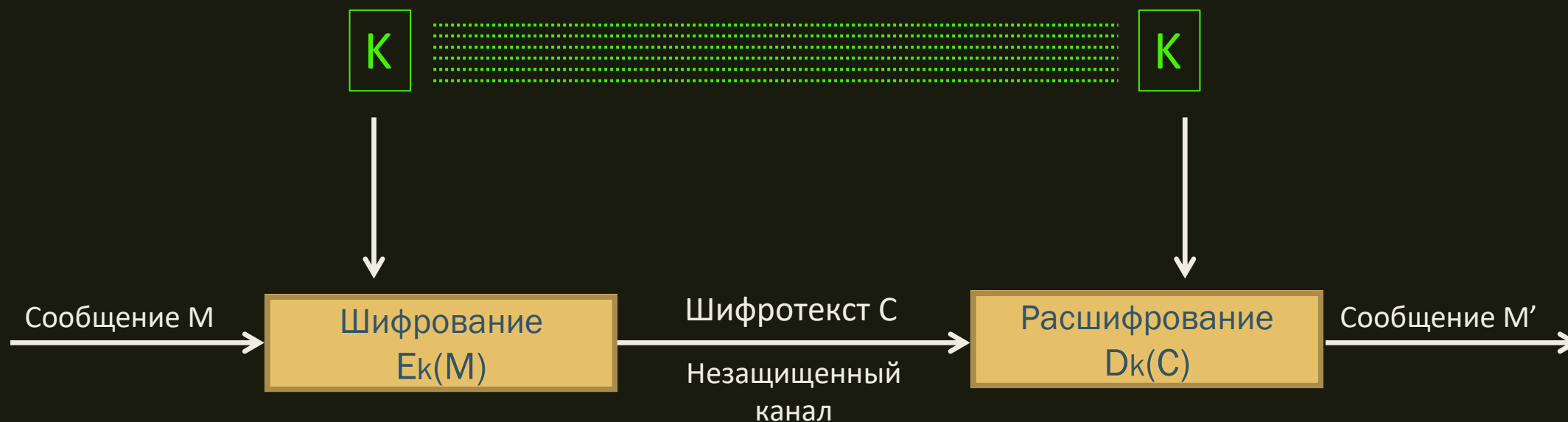
Алгоритм Диффи-Хеллмана



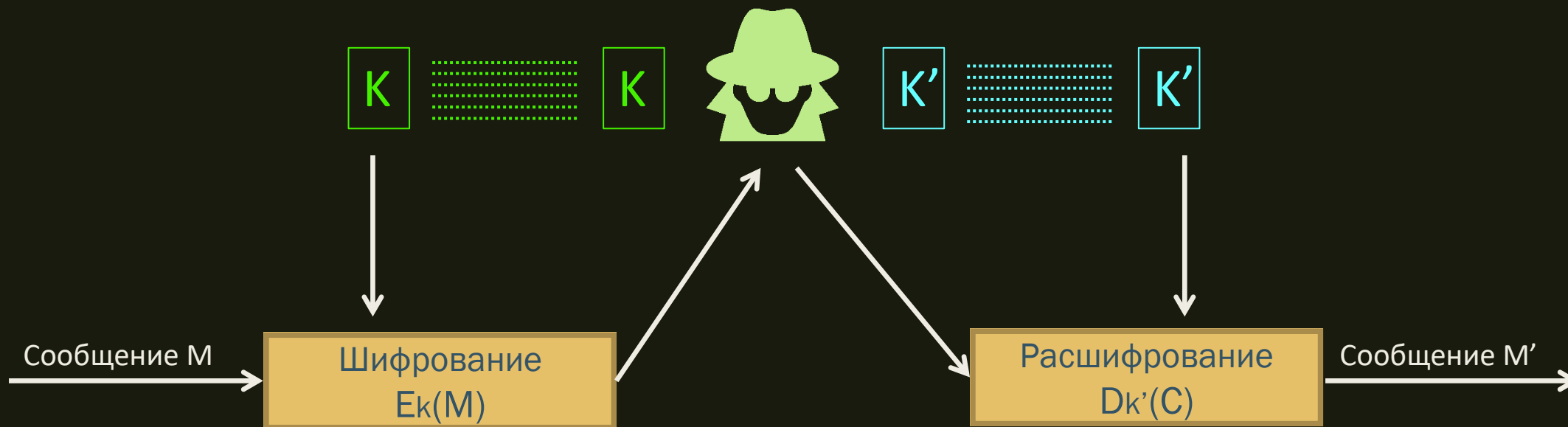
Практика



Безопасная передача...



MITM - men in the middle





RSA

RSA

Rivest, Shamir, Adleman

Криптографический алгоритм шифрования с открытым ключом

Публичный ключ

e

$$M + e \rightarrow Se$$

$$Se + d \rightarrow M$$

$$Se + e \rightarrow \text{Error}$$

Закрытое одним
открывается другим

d

Приватный ключ

$$M + d \rightarrow Sd$$

$$Sd + e \rightarrow M$$

$$Sd + d \rightarrow \text{Error}$$

Основы алгоритма

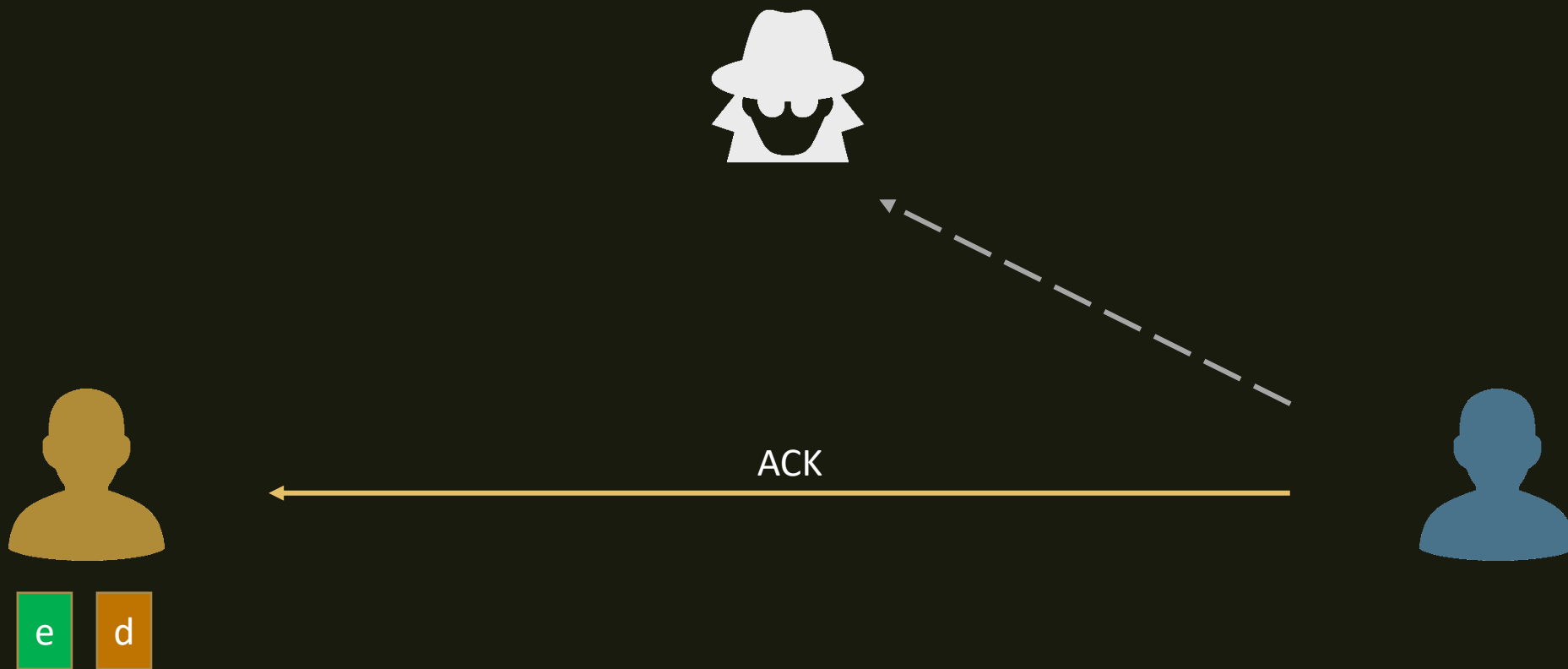


e

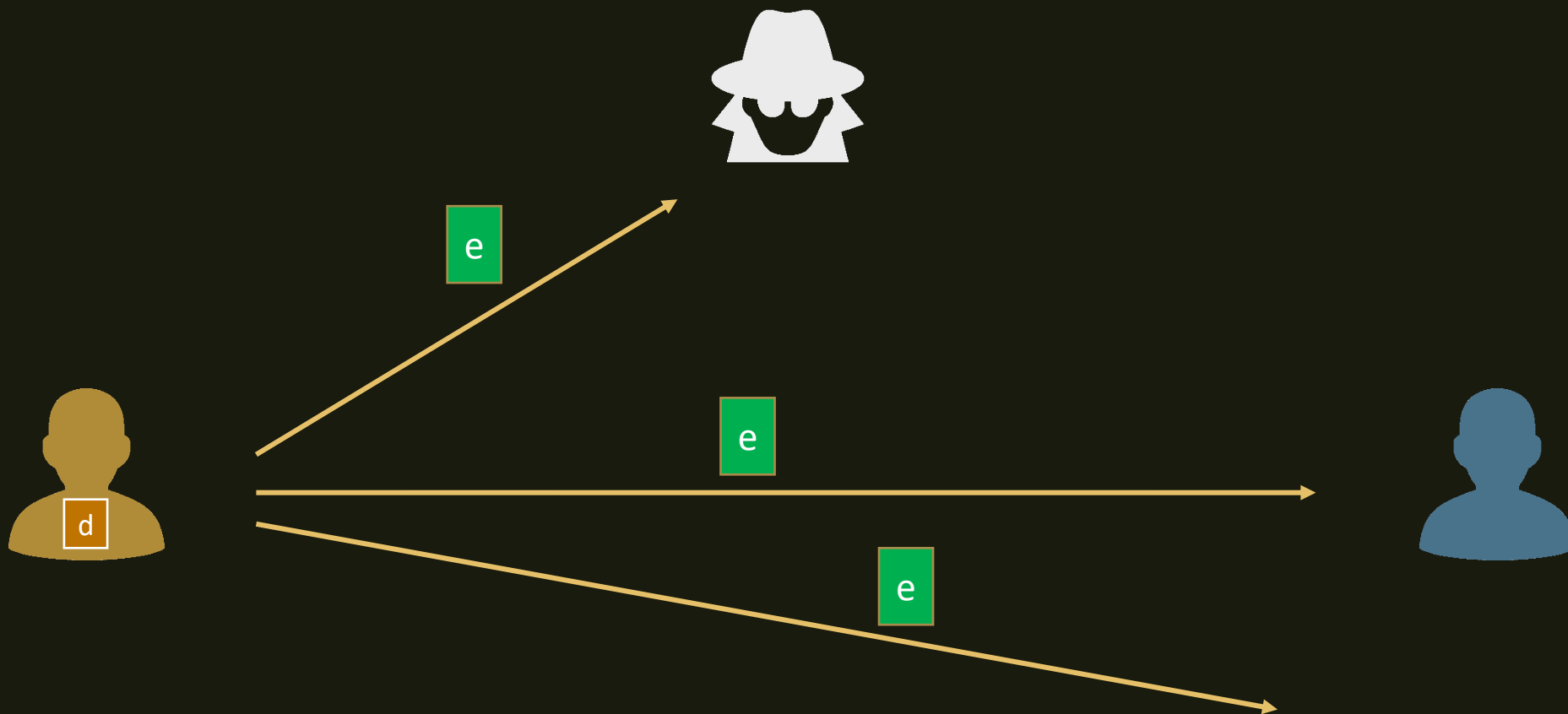
d



Основы алгоритма



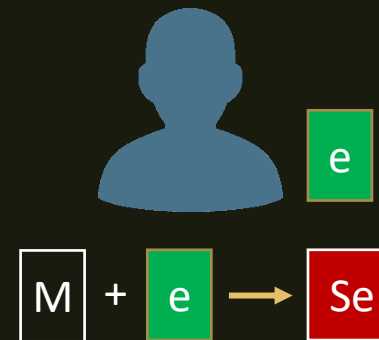
Основы алгоритма



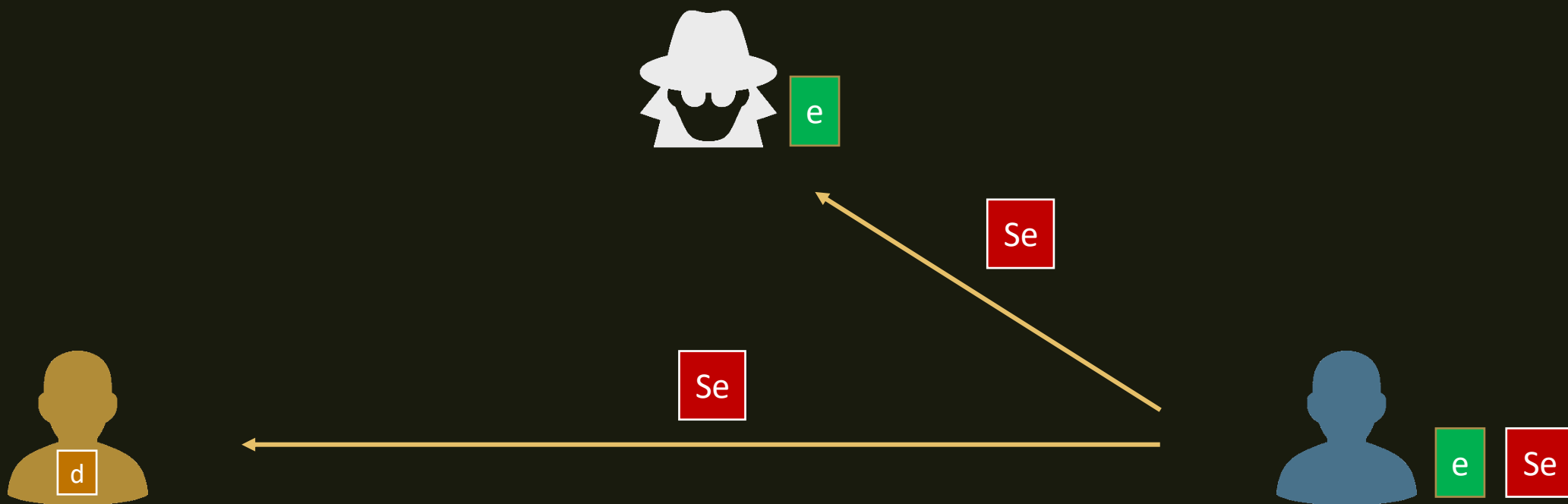
Основы алгоритма



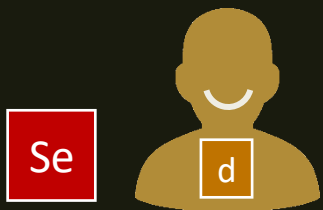
Основы алгоритма



Основы алгоритма



Основы алгоритма



Генерация ключей RSA

①

Выбрать два простых числа p и q

p, q

②

Вычислить модуль n

$$n = p * q$$

n

③

Вычисляем Функцию Эйлера

$$F(n) = (p - 1) * (q - 1)$$

$F(n)$

④

Выбрать любое такое число e , что:

- взаимно простое с $F(n)$
- меньше, чем $F(n)$

e

⑤

Определить такое d , чтобы:

$$(d * e) \bmod F(n) = 1$$

d



d e n

Публичный ключ

Приватный ключ



d e n

Публичный ключ

e n

Приватный ключ

d n

d e n

Публичный ключ

e n

$$M^e \bmod n = S^e$$

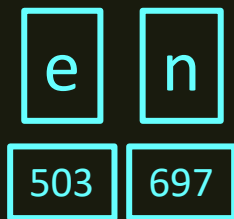
Приватный ключ

d n

$$S^e \bmod n = M$$

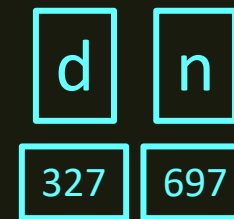


Публичный ключ



$$M^e \bmod n = Se$$

Приватный ключ



$$Se^d \bmod n = M$$

Публичный ключ

e	n
503	697

$$M^e \bmod n = Se$$

$$13^{503} \bmod 697 = 140$$

Приватный ключ

d	n
327	697

$$Se^d \bmod n = M$$

$$140^{327} \bmod 697 = 13$$

e

n



$$140^{503} \bmod 697 = 540$$

$$140^{503} =$$

8112211523730376553870495507653403628354949114652588682980196328348076240324281569276238884322041382771605077697154987855727608899125767220212269513609016
28667600229592997813684671219067015620519405789796484314401629632571905931480407819571324903832357351700360812577452087679145917361331050653387922706829561
857685330768790399671588556669112434408568572077763724296534566032128596124207889730434655...

1159 цифр

Публичный ключ

e n

503 697

$$M^e \bmod n = S_e$$

$$13^{503} \bmod 697 = 140$$

Приватный ключ

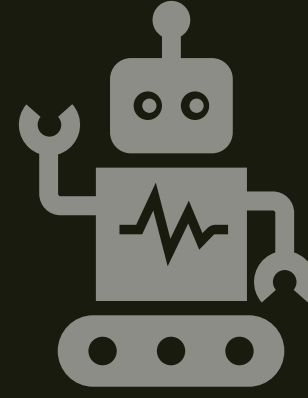
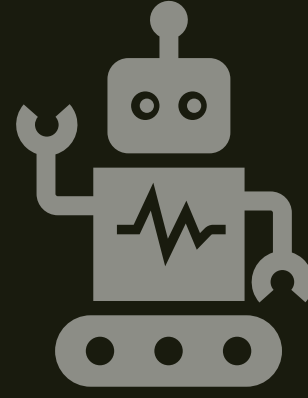
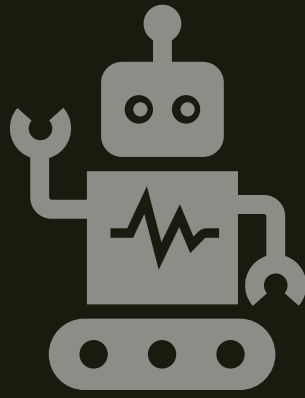
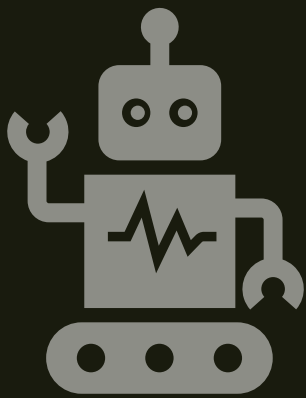
d n

327 697

$$S_e^d \bmod n = M$$

$$140^{327} \bmod 697 = 13$$

Практика



ФИО	e	n	$777^d \bmod n$
-----	---	---	-----------------