v. 2.0

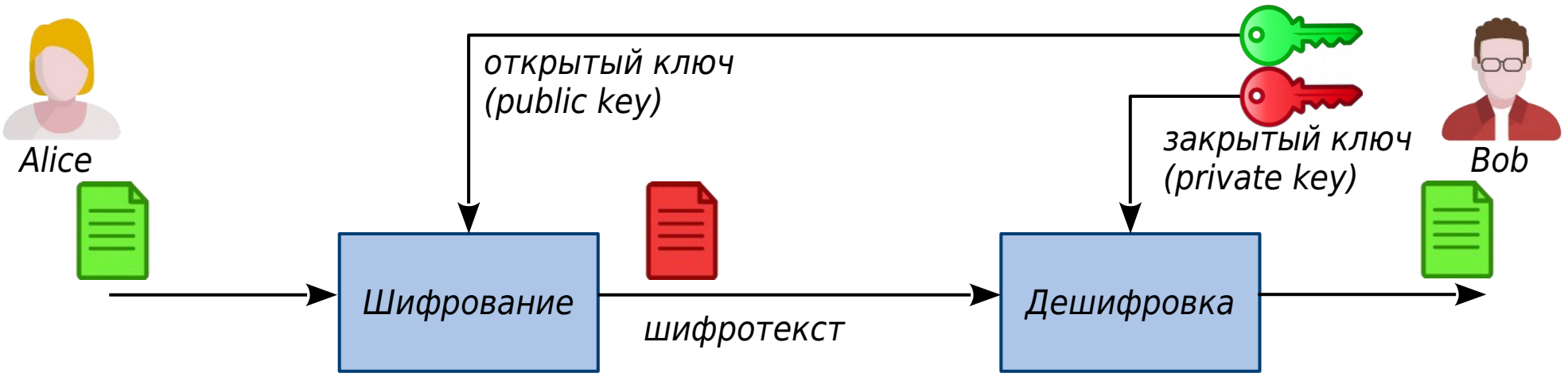
Криптография

Лекция 2. Асимметричные шифры.

Дмитрий Яхонтов

“Кочерга”, 2019

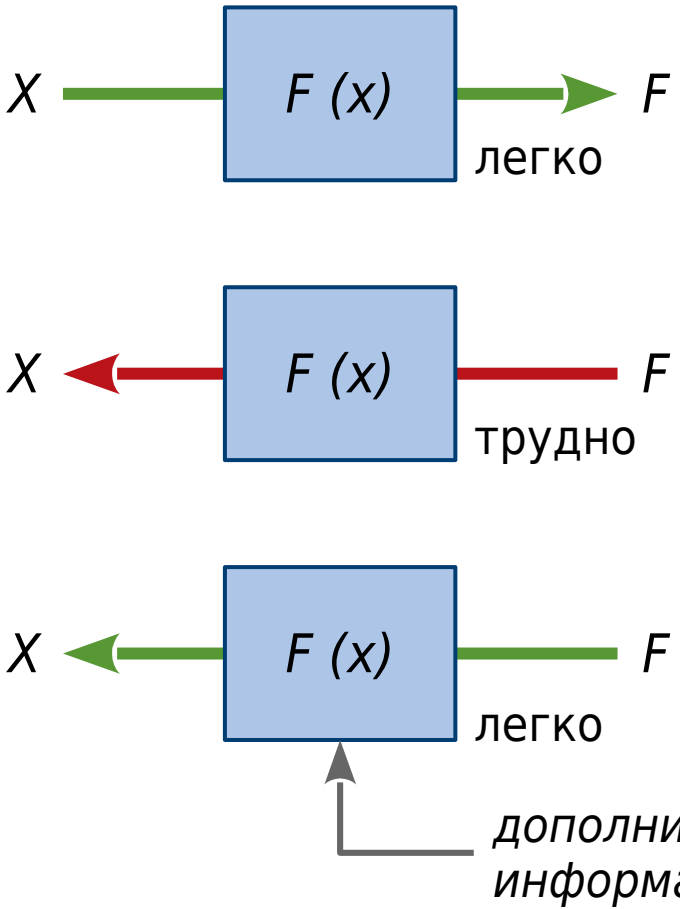
Асимметричное шифрование
(оно же шифрование с открытым ключом)



Для шифрования и дешифровки служат разные ключи.

Открытый ключ распространяется свободно,
закрытый необходимо сохранять в секрете.

Односторонние функции



- В прямом направлении функция вычисляется легко (с полиномиальной сложностью).
- Не существует *известного* алгоритма для лёгкого вычисления функции в обратном направлении.
- Функция с “потайным входом”: знание дополнительной информации позволяет легко вычислить функцию в обратном направлении.

Протокол Диффи — Хеллмана
(пример с цветами)

Alice

Bob

открытый цвет

X → X

A + X → A+X → A+X

секретный цвет

секретный цвет

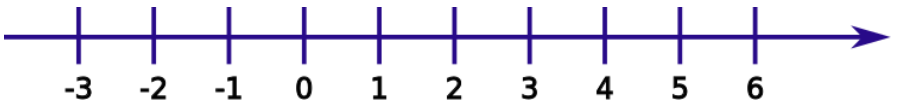
B+X ← B+X ← X + B

A + B+X → A+B+X

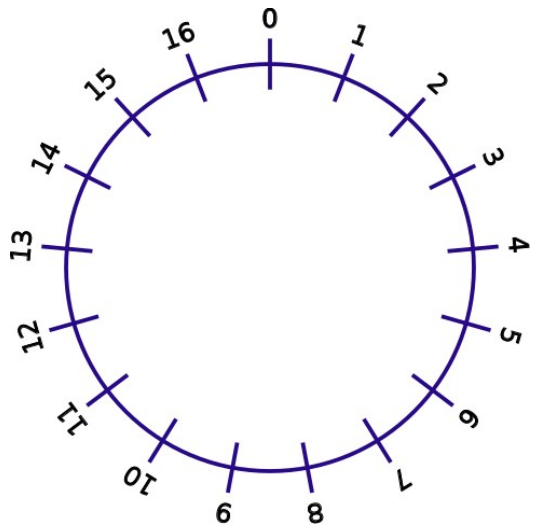
общий ключевой цвет

B+A+X ← A+X + B

Модулярная арифметика



Z *— целые числа*



Z/n *— целые числа по модулю n*

- *Сравнение по модулю*
  $A \bmod n = X$:
  $0 \le X \le n-1$
  $A = kn + X$
- *Обратное число* X^{-1}
  $X \cdot X^{-1} \bmod n = 1$
- *Вычисление обратных чисел — расширенный алгоритм Евклида*

Протокол Диффи — Хеллмана

Alice

Eve

$g^a \bmod n$

$g^b \bmod n$

$g^{ab} \bmod n = ?$

Bob

простое **n** → **n**

открытое число **g** → **g**

секретное число **a** — **b** *секретное число*

A = $g^a \bmod n$ → **A**

B ← **B** = $g^b \bmod n$

K = $B^a \bmod n$ =
= $g^{ba} \bmod n$

K = $A^b \bmod n$ =
= $g^{ab} \bmod n$

Протокол RSA

Alice

Eve

$m^e \bmod n$

n, e

m = ?

Bob

p, **q** — *секретные простые*

n = pq

n

открытый ключ:

e *взаимно простое с* (p–1)(q–1)

e

сообщение **m**

закрытый ключ:

$\mathbf{d} = e^{-1} \bmod ((p-1)(q-1))$

шифрование:

$\mathbf{C} = m^e \bmod n$

C

дешифровка:

$\mathbf{D} = C^d \bmod n = m^{ed} \bmod n = m$

Почему это работает?

- *функция Эйлера:*

  $\boldsymbol{\varphi(n)}$ *— количество натуральных чисел меньше n, взаимно простых с ним*

  для простых чисел: $\varphi(\mathbf{p}) = \mathbf{p}-1$; $\varphi(\mathbf{q}) = \mathbf{q}-1$

  функция Эйлера мультипликативна: $\varphi(\mathbf{n}) = \varphi(\mathbf{pq}) = \varphi(\mathbf{p})\varphi(\mathbf{q}) = (\mathbf{p}-1)(\mathbf{q}-1)$

- *теорема Эйлера:* $\mathbf{x}^{\varphi(\mathbf{n})} = 1 \bmod \mathbf{n}$ *для взаимно простых* ***n*** *и* ***x***

- *доказательство корректности дешифровки RSA:*

  $\mathbf{e}\cdot\mathbf{d} = 1 \bmod \varphi(\mathbf{n}) = 1 + a\cdot\varphi(\mathbf{n})$

  сообщение после шифрования и дешифровки:

  $\mathbf{m}^{\mathbf{ed}} = \mathbf{m}^{(1 + a\cdot\varphi(\mathbf{n}))} = \mathbf{m}^1 \cdot \mathbf{m}^{a\cdot\varphi(\mathbf{n})} = \mathbf{m} \cdot \underbrace{(\mathbf{m}^{\varphi(\mathbf{n})})^{\mathbf{a}}} \bmod \mathbf{n} = \mathbf{m} \cdot 1$

  по теореме Эйлера вот это равно 1

Протокол RSA
(пример с числами)

Alice

Bob

p = 7, **q** = 13

n = 7·13 = 91

n = 91 ←

открытый ключ:

e = 5

e = 5 ←

сообщение

m = 24

закрытый ключ:

d = 5^{-1} mod (6·12) = 29

29·5 = 145 = 1 mod 72

шифрование:

C = 24^5 mod 91=

= 7 962 624 mod 91=

= 33

→

дешифровка:

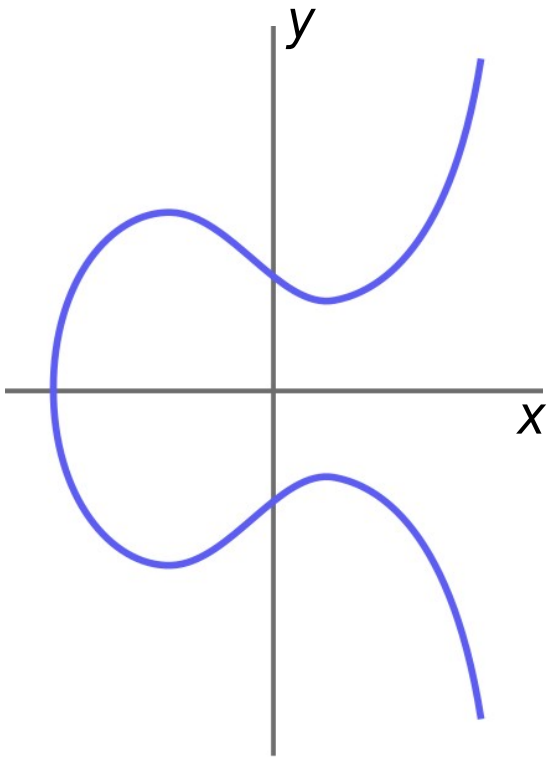
D = 33^{29} mod 91 =

108 869 005 682 301

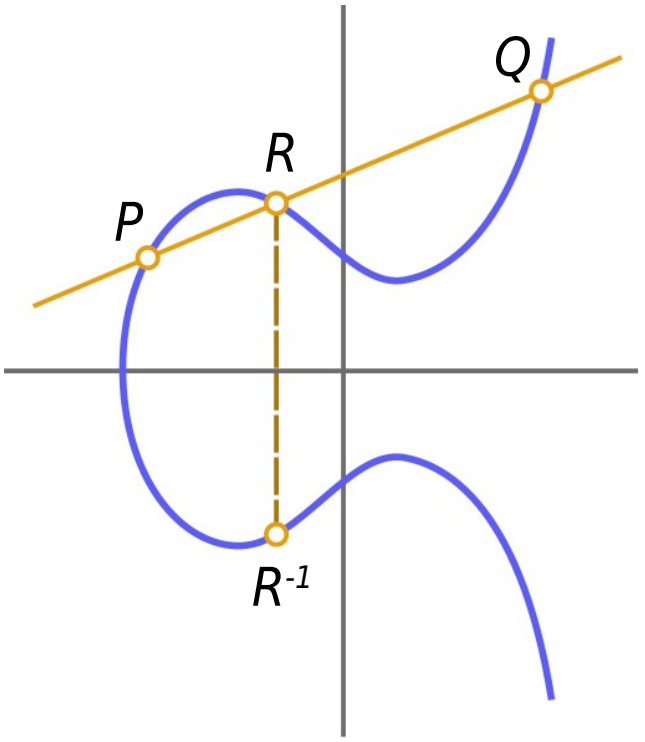
795 684 211 705 446

369 982 097 742 753 mod 91 = 24

Криптография на эллиптических кривых



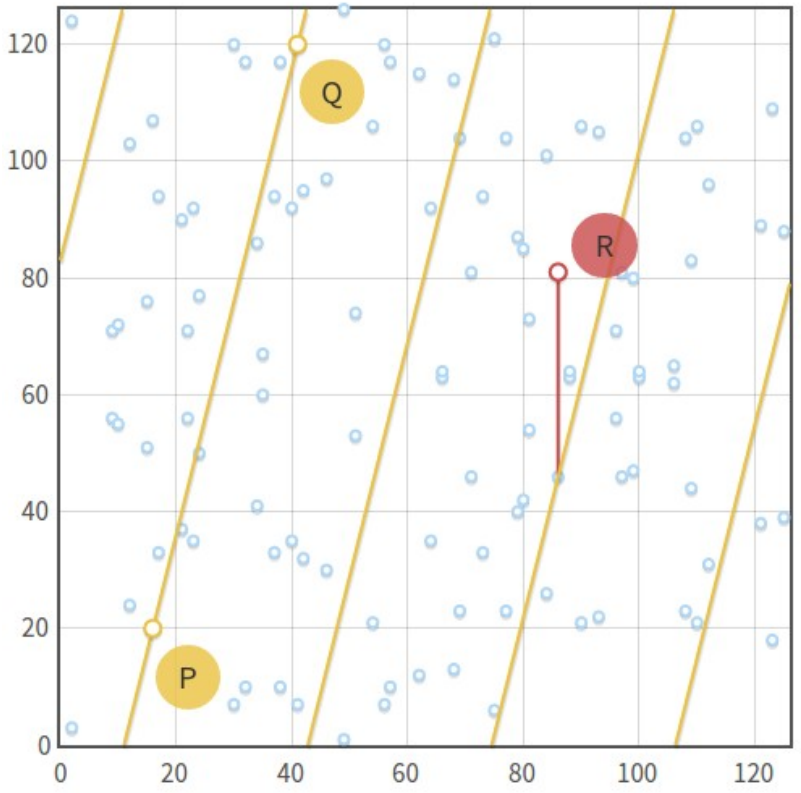
$y^2 = x^3 + ax + b$



- *Определим 1*
  $P * 1 = P$
- *Определим* P^{-1}
  $P * P^{-1} = 1$
- *Определим операцию* *
  $P * Q * R = 1$
  если P, Q, R лежат на одной прямой.

  $P * Q = R^{-1}$

Эллиптические кривые над полем целых чисел по модулю *n*



$y^2 = (x^3 + ax + b) \bmod n$

- Координаты точек — целые числа от 0 до (n–1)
- Все определения работают:

  $P * 1 = P$
  $P * P^{-1} = 1$
  $P * Q = R^{-1}$

- Возведение в степень:

  $P^k = P * P * P * \ldots * P$ *(k раз)*

- Обратная задача (дискретный логарифм) — трудная.

название системы	год	вычислительная задача	назначение
Диффи — Хеллмана	1976	дискретный логарифм	обмен ключами
RSA (Rivest-Shamir-Adleman)	1977	разложение на простые множители	шифрование, ЭЦП
Меркла — Хеллмана	1978	задача о рюкзаке	шифрование
Рабина	1979	дискретный квадратный корень	шифрование
DSA (Digital Signature Algorithm)	1991	дискретный логарифм	ЭЦП
ECDSA (Elliptic Curve Digital Signature Algorithm)	1999	дискретный логарифм на эллиптич. кривых	ЭЦП
ГОСТ Р 34.10-2012	2012	дискретный логарифм на эллиптич. кривых	ЭЦП
NTRUEncrypt	1996	поиск кратчайшего вектора решётки	шифрование, ЭЦП

Преимущества и недостатки
(по сравнению с симметричной криптографией)

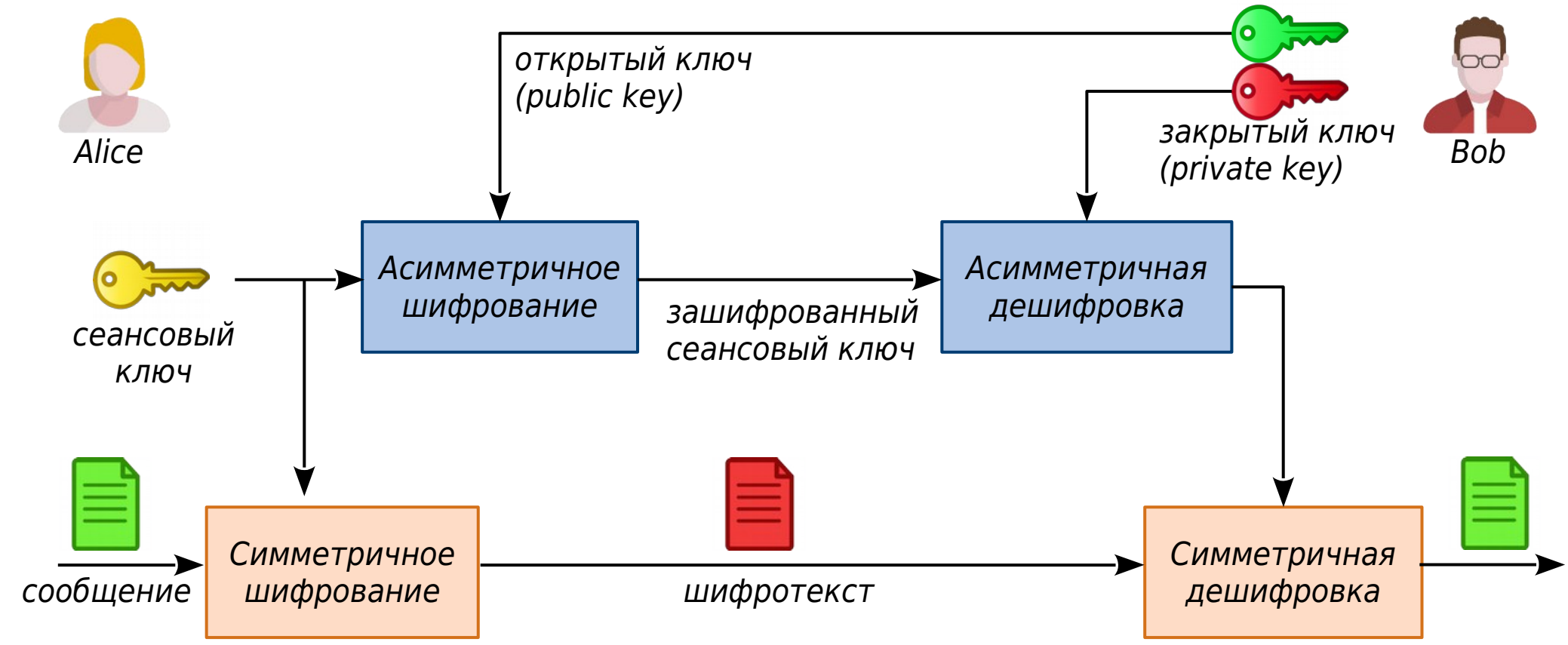
Преимущества:

- Не нужен защищённый канал для передачи ключей
- Только одна сторона должна хранить ключ в секрете
- Простой обмен ключами в сетях с большим числом участников
- Возможность создания цифровой подписи

Недостатки:

- Ресурсоёмкие и медленные (в ~1000 раз) алгоритмы
- Требуется большая длина ключа (в ~5–20 раз)
  для достижения сравнимой стойкости

Гибридное шифрование



Криптоанализ асимметричных шифров

- Метод “baby-step, giant-step”

$Q = P^x \bmod n, \; x = ?$

$Q = P^{(am+b)}$

$Q = P^{am} * P^b$

$Q * (P^{am})^{-1} = P^b$

$m = \sqrt{n}$

1. Для всех b = 0, 1, 2 ... m: вычисление P^b *(baby step)*
2. Для всех a = 0, 1, 2 ... m: вычисление $Q * (P^{am})^{-1}$ *(giant step)*
3. Поиск совпадений между результатами п.1 и 2

Вместо полного перебора со сложностью 2^n перебор двух диапазонов со сложностью $2^{(n/2+1)}$ и использование памяти объемом $2^{(n/2)}$

- ## Поиск слабых классов параметров

  Для некоторых частных случаев существуют алгоритмы быстрого вычисления обратной функции. Параметры криптосистемы, позволяющие применять эти алгоритмы, называются **слабыми**.

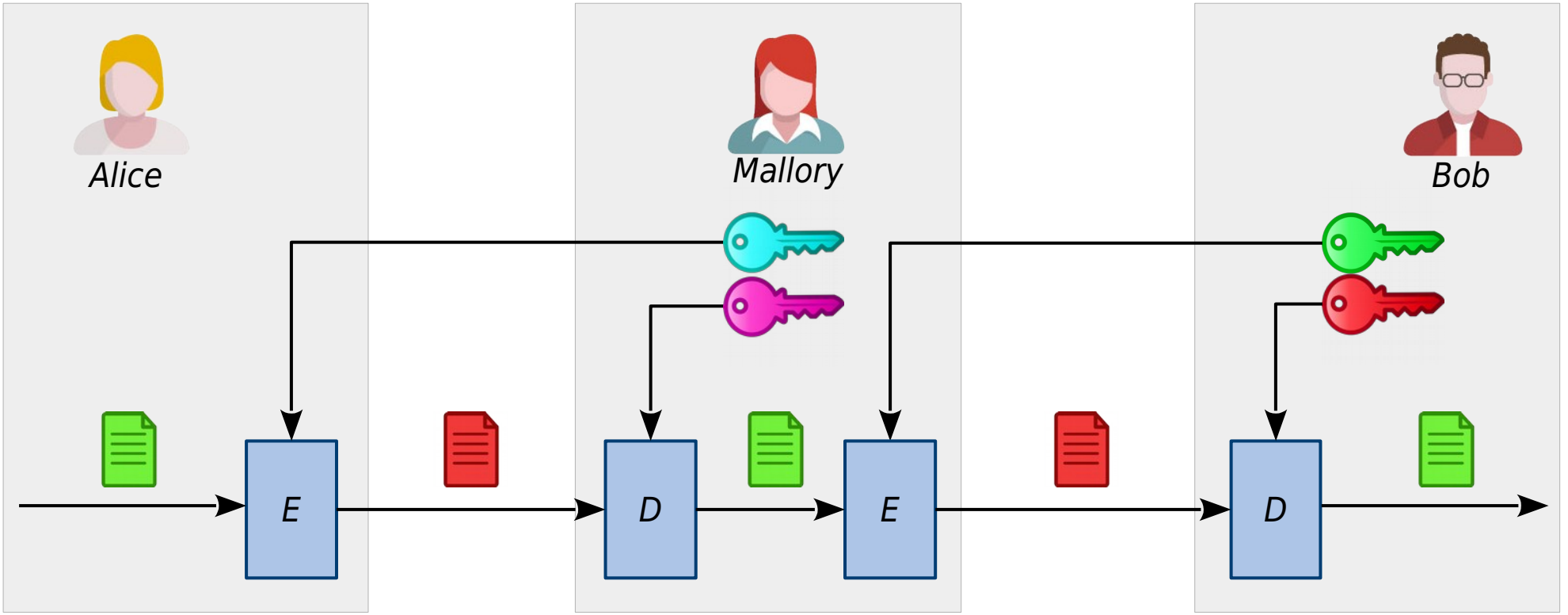
  Например: слабые ключи, слабые эллиптические кривые.

  Принцип проверяемой случайности (*“nothing up my sleeve”*)

  S = random() ⟶ односторонняя функция ⟶ параметры

  Вместе с параметрами системы публикуется порождающее значение S. Односторонняя функция гарантирует, что S не может быть вычислено постфактум, на основе подобранных слабых параметров.

Атака “человек посередине”
(Man-in-the-Middle, MitM)



Задачи

1. Предложите модификацию протокола Диффи—Хеллмана для произвольного числа участников (больше двух).
   Все участники должны получить общий секретный ключ.
2. Алиса — провайдер кабельного телевидения — предоставляет услугу “фильм по запросу”. Абонент (Боб) выбирает фильм по каталогу, затем шифрует название фильма и желаемое время просмотра по протоколу RSA открытым ключом Алисы и отправляет ей. В указанное время Алиса начинает трансляцию фильма по кабельной сети всем абонентам сразу.

   Ева может прослушивать линии связи абонентов, и она очень хочет узнать, кто какие фильмы заказывает. Предложите способ это сделать. Какие изменения нужно внести в протокол, чтобы противодействовать данной атаке?

Ссылки

- Обратная связь:
  - android.ruberoid@gmail.com
  - @androidruberoid
- Анонсы:
  - facebook.com/kocherga.club
  - vk.com/kocherga_club
  - vk.com/kocherga_prog
- Материалы лекций:
  - github.com/notOcelot/Kocherga_crypto
- Видео:
  - youtube.com/channel/UCeLSDFOndl4eKFutg3oowHg