

# КРИПТОСИСТЕМА ЭЛЬ-ГАМАЛЯ

ПОДГОТОВИЛ СТУДЕНТ 2 КУРСА НИУ ВШЭ

СИДОРЕНКОВ ОЛЕГ, БПИ204





# ПЛАН ПРЕЗЕНТАЦИИ

- Дискретное логарифмирование с примерами
- Протокол Диффи — Хеллмана с примерами
- История создания схемы Эль-Гамала
- Алгоритм Эль-Гамала
- Примеры шифрования / расшифрования
- Интересные факты

# ДИСКРЕТНОЕ ЛОГАРИФИРОВАНИЕ

Пусть есть конечная абелева группа  $G$

Пусть есть элемент  $b \in G$

Пусть есть  $y \in G$

Рассмотрим уравнение  $y = b^x$

Если оно разрешимо, то  $\exists x < \text{ord}(G)$ ,  $x \in \mathbb{N}$

Пример:

Рассмотрим группу  $Z_5$

$$b = 3$$

$$y = 2$$

$$2 = 3^x \bmod 5$$

$$b^3 = 27 \bmod 5 = 2$$

$$x = 3$$



# ПРОТОКОЛ ДИФФИ-ХЕЛЛМАНА

Протокол Диффи-Хеллмана — криптографический протокол (набор крипто-алгоритмов), позволяющий двум и более сторонам получить общий секретный ключ, используя незащищенный от прослушивания канал связи. Полученный ключ используется для шифрования дальнейшего обмена с помощью алгоритмов симметричного шифрования.

## Алгоритм:

Пусть есть 2 пользователя: Алиса и Боб

Возьмём 2 общеизвестных числа  $g$  и  $p$

Оба человека генерируют 2 больших неизвестных никому случайных числа  $a$  и  $b$  соответственно

Алиса находит остаток от деления:

$$A = g^a \bmod p$$

Далее пересылает результат Бобу

Боб тоже вычисляет остаток от деления:

$$B = g^b \bmod p$$

Передаёт Алисе

Оба этих значения могут передаваться по незащищённому каналу связи

Алиса повторяет свои действия с новым числом  $B$ :

$$C = B^a \bmod p = g^{ab} \bmod p$$

Боб всё делает зеркально:

$$C = A^b \bmod p = g^{ab} \bmod p$$

У обоих получилось одно и тоже число  $C$ , которое и является ключом. Его будет трудно найти за конечное время

P. S. Фактически, мы работали в поле  $F_p$

# ПРИМЕР АЛГОРИТМА

Возьмём числа  $p = 23$  и  $g = 5$

Алиса и Боб сгенерили числа  $a = 6$  и  $b = 15$

$A = 5^6 \bmod 23 = 8$

$B = 5^{15} \bmod 23 = 19$

У Алисы  $K = 19^6 \bmod 23 = 2$

У Боба  $K = 8^{15} \bmod 23 = 2$



# ИСТОРИЯ ШИФРА ЭЛЬ-ГАМАЛЯ

Тахер Эль-Гамаль родился в 1955 году в Каире. С детства будущий криптограф любил производить всевозможные операции над числами, поэтому не удивительно, что в будущем, во время обучения в Стенфордском университете он увлёкся линейной алгеброй. В 1985 году опубликовал статью под названием «Криптосистема с открытым ключом и схема цифровой подписи на основе дискретных логарифмов». Эта работа в последствии была названа криптосистемой или шифром Эль-Гамала, позднее дополнившись цифровой подписью с аналогичным названием.



Тахер Эль-Гамаль  
Род. 18.06.1955, 66 лет



# АЛГОРИТМ ШИФРА ЭЛЬ-ГАМАЛЯ

Шифр Эль-Гамала – это один из способов выработки ключей Диффи-Хеллмана.

Ключи:

$p$  – некоторое простое число

$$g^{\varphi(p)} \equiv 1 \pmod{p}$$

Так как  $p$  – простое, то  $\varphi(p) = p - 1$

$$g^{p-1} \equiv 1 \pmod{p}$$

Берём  $x \in (1; p - 1)$

Вычисляем  $y = g^x \pmod{p}$

Получаем открытые ключи  $(y, g, p)$  и закрытый ключ  $x$

Зашифровка:

Пусть есть сообщение (число)  $M < p$

Выбираем ключ  $k$ , взаимно простой с

$p - 1$ , причём  $k \in (1; p - 1)$

Вычисляем два числа  $a$  и  $b$ :

$$a = g^k \pmod{p}$$

$$b = y^k \cdot M \pmod{p}$$

Пара  $(a, b)$  и является зашифрованным сообщением.

Расшифровка:

Рассмотрим формулу  $M = ba^{-x} \pmod{p}$

Докажем её правильность

$$a = g^k \pmod{p} \rightarrow a^{-x} = g^{-kx} \pmod{p}$$

$$b = y^k \cdot M \pmod{p}$$

$$ba^{-x} = y^k \cdot M \cdot g^{-kx} \pmod{p}$$

$$y = g^x \pmod{p}$$

$$ba^{-x} = g^{kx} \cdot M \cdot g^{-kx} \pmod{p} = M$$

$$M = ba^{-x} \pmod{p} = ba^{p-x-1} \pmod{p}$$

# ЦИФРОВАЯ ПОДПИСЬ ЭЛЬ-ГАМАЛЯ

Цифровая подпись – это элемент обмена сообщений, который может подтвердить подлинность источника. Предполагается, что у нас в распоряжении есть некая хеш-функция  $h(\cdot)$ , причём результаты её выполнения  $\in (1, p - 1)$

Подпись сообщения:

Пусть есть сообщение  $M$

Вычисляем хеш-сумму

$$m = h(M)$$

Берём случайное  $k \in (1, p - 1)$

Причём  $k$  и  $p - 1$  являются взаимнопростыми

$$\text{Вычисляем } r = g^k \bmod p$$

$$\text{И } s = (m - x \cdot r) \cdot k^{-1} \bmod p - 1$$

$k^{-1}$  – это такое целое число,

$$\text{что } k \cdot k^{-1} = k^{-1} \cdot k = 1 \bmod p - 1$$

Подписью является пара чисел  $(r, s)$

Проверка подписи:

Сначала проверим, что

$$r \in (0; p), \text{ а } s \in (0; p - 1)$$

Если всё хорошо, вычисляем хеш-сумму  $m = h(M)$

Подпись считается верной при выполнении равенства:

$$y^r \cdot r^s \equiv g^m \pmod{p}$$

Особенности данной подписи:

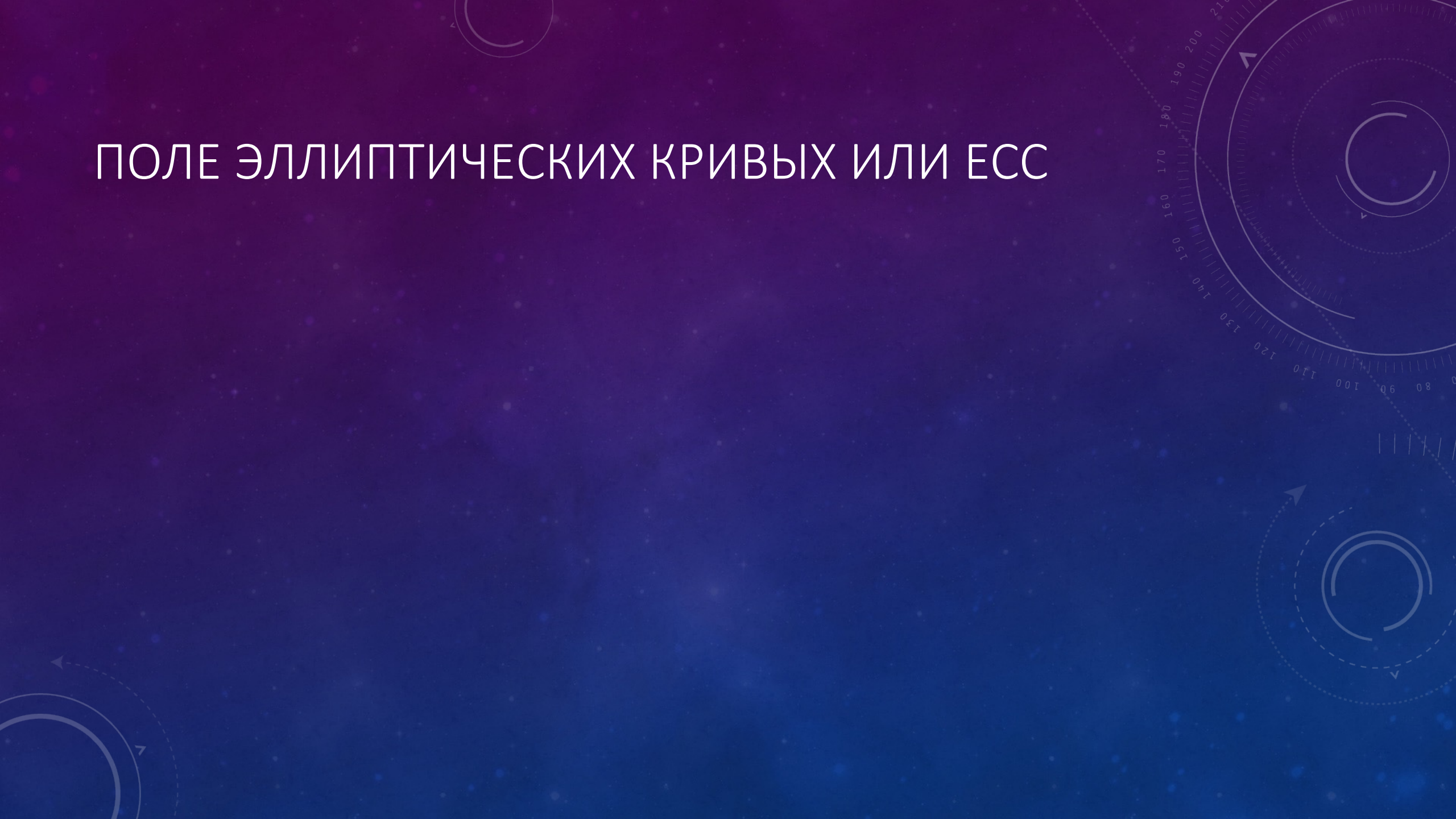
Главным преимуществом схемы цифровой подписи Эль-Гамала является возможность вырабатывать цифровые подписи для большого числа сообщений с использованием только одного секретного ключа.

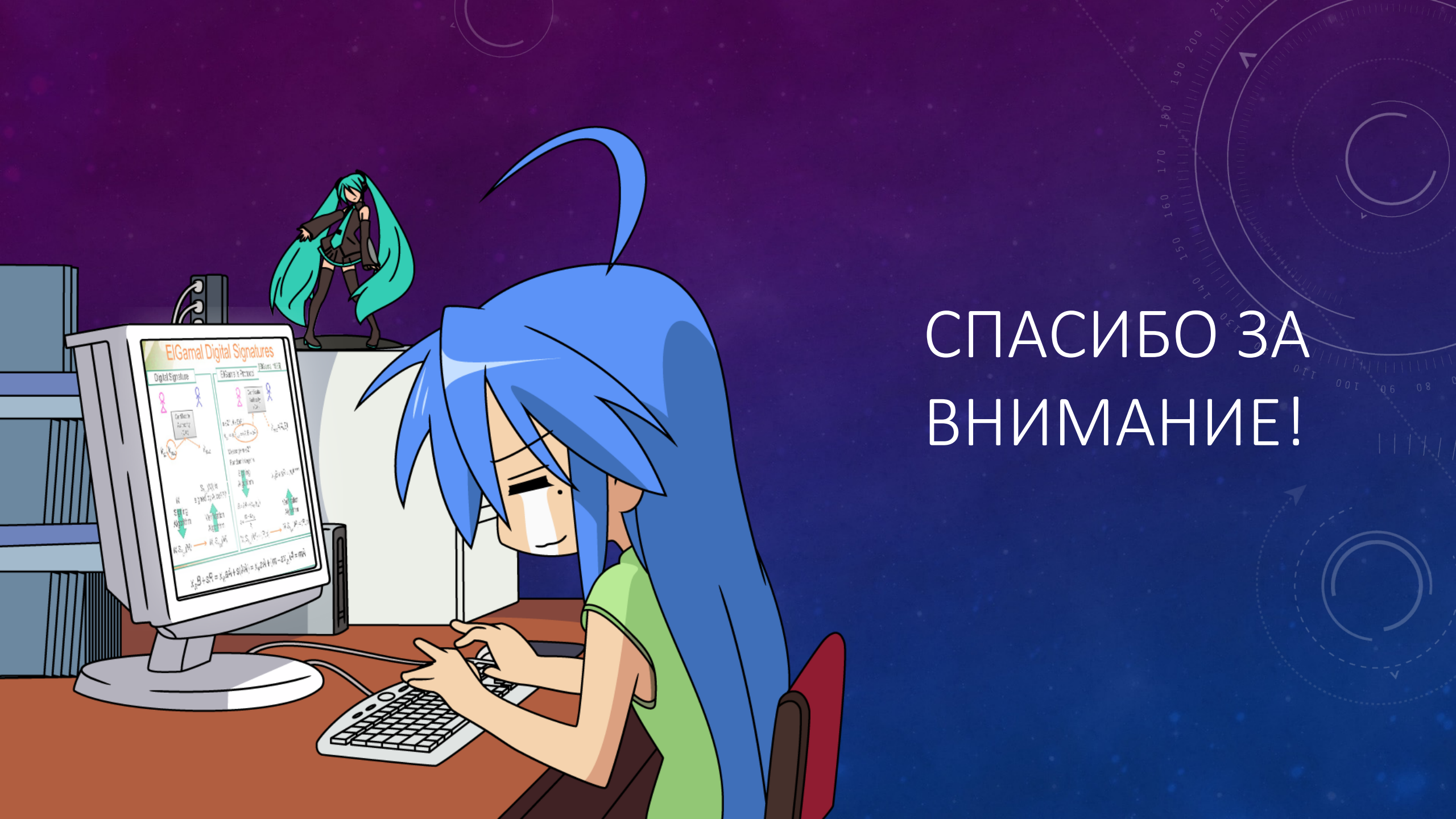
Нельзя допустить утечки ключа  $k$ , так как злоумышленник сможет найти секретный ключ:  $x = (m - k \cdot s) \cdot r^{-1} \bmod p - 1$ .

На принципе Эль-Гамала построены стандарты цифровой подписи США и России.



# ПОЛЕ ЭЛЛИПТИЧЕСКИХ КРИВЫХ ИЛИ ЕСС





СПАСИБО ЗА  
ВНИМАНИЕ!