Основы криптографии

Введите подзаголовок

Кто я?

Подпись к картинке

1. Математик со стажем 8 лет. Матан
2. Криптограф со стажем 4 года.

4. Питона не существует, есть только sage

Слайд для оценки аудитории

История

- Появилась давно
- Сокрытие информации придумали сразу же после того, как придумали двери
- Пришли математики и вернулись физики
- Сделали магию

Сегодня

- Конфиденциальность
- Доступность
- Буст математики и информатики
- Буст экономики(чуток)
- Буст физики

Криптосистема

K - пространство ключей
M - пространство открытых текстов
C - пространство шифротекстов
e - функция шифрования
d - функция расшифрования

$$e : K \times M \to C$$

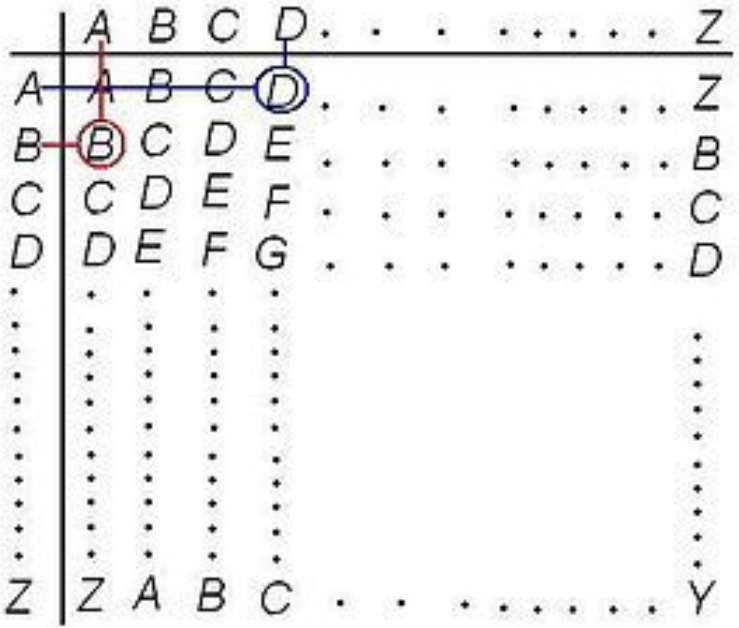
$$d : K \times C \to M$$

$$d(e(K, m), c) = m$$

$$e(d(K, c), m) = c$$

База по Цезарю

ключ	A B C A B C
открытый текст	D A N C E
шифрованный текст	D B P C F



Примитивы

Генераторы псевдослучайных чисел

- Криптографически стойкие и не очень

- В основном базируются на lfsr (Регистр сдвига с линейной обратной связью) и в целом на рекуррентах

- Могут быть на основе потоковых шифров

- LCG, MT, RC4...

Перемешиваем

Хе(э)ш функции

- Быстро считается, сложно обращается
- Почти односторонние отображения
- Берут в себя много, возвращают фиксировано
- sha1, sha2, sha3, md

Крипто типы

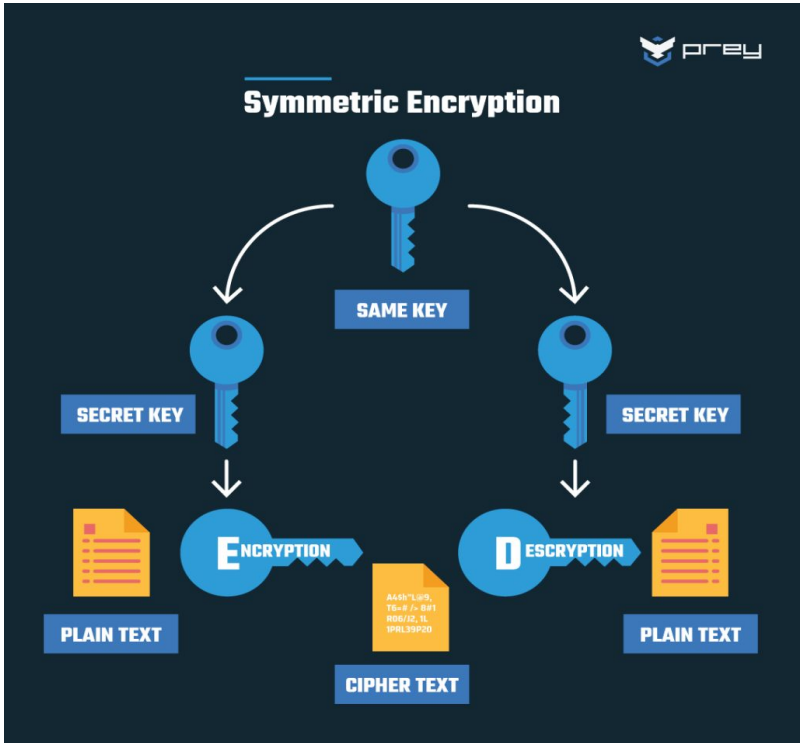
Два типа криптографии

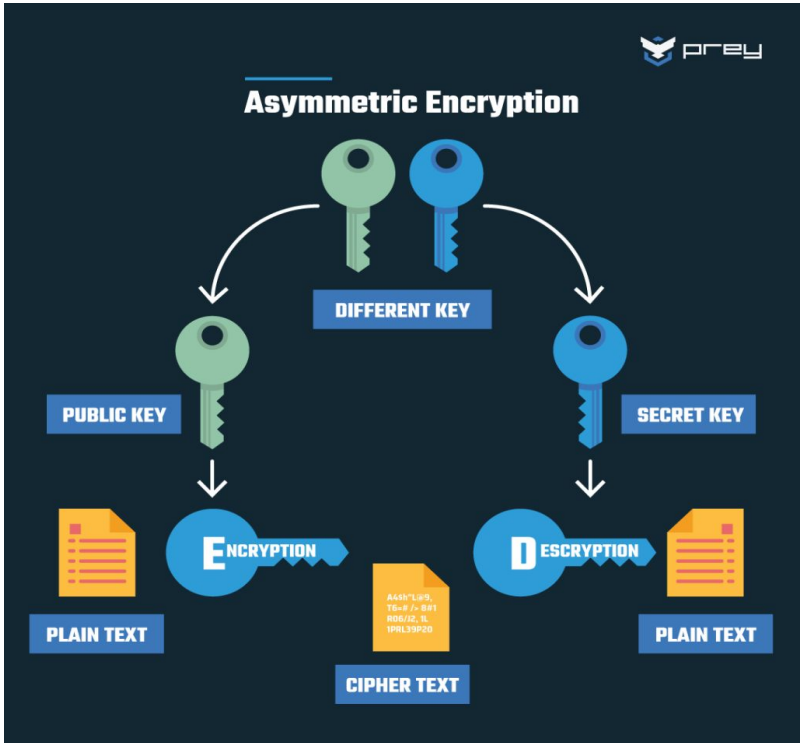
Симметричная

1. Ключ для шифрования и расшифрования один и тот же
2. Быстро
3. Нужен предварительный обмен ключами

Ассиметричная

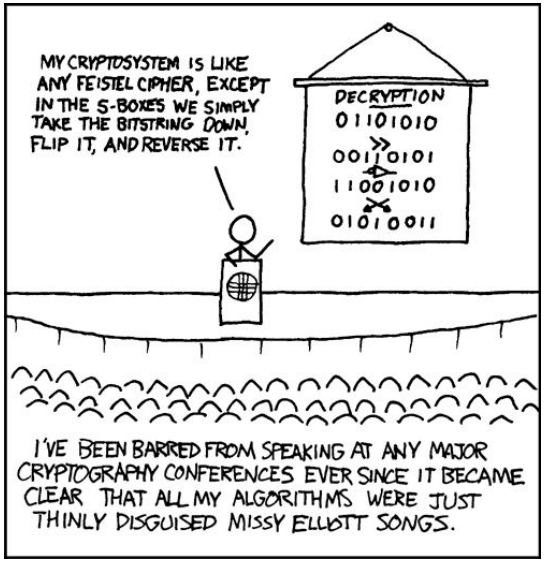
1. Ключи разные
2. Не так быстро, а иногда даже совсем
3. Обмен ключами может быть произведен по открытому каналу связи


prey
Symmetric Encryption
SAME KEY
SECRET KEY
SECRET KEY
ENCRYPTION
DESCRYPTION
PLAIN TEXT
PLAIN TEXT
CIPHER TEXT


prey
Asymmetric Encryption
DIFFERENT KEY
PUBLIC KEY
SECRET KEY
ENCRYPTION
DESCRYPTION
PLAIN TEXT
PLAIN TEXT
CIPHER TEXT

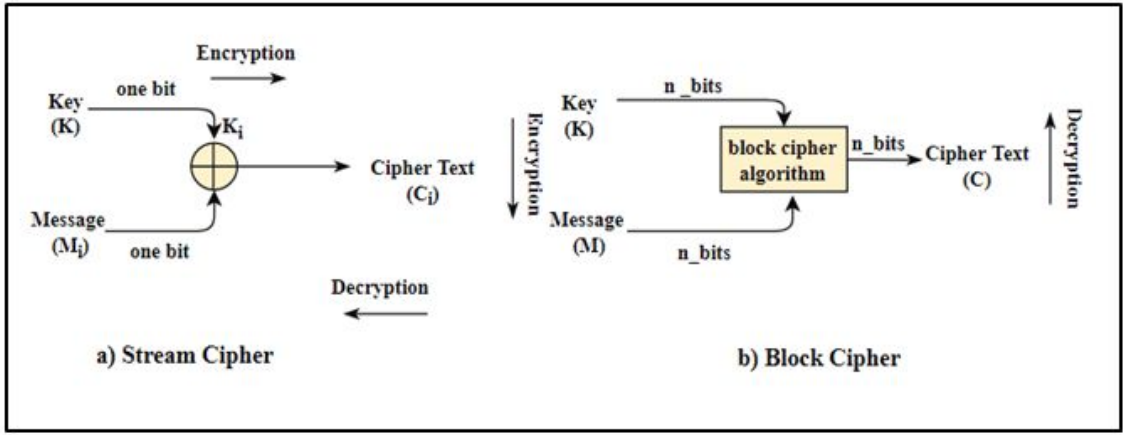
Симметричное шифрование

- Булевы функции, S-boxы и много-много битов
- Цезарь, Виженер, OTP, AES, DES, ChaCha20, RC4, Feistel...



Типы симметричных шифров

- Блочный. AES, DES
- Потоковый. RC4, ChaCha20



Режимы блочных шифров

- ECB
- CBC
- CTR
- GCM

Подходы к анализу

- Частотный анализ
- Линейный анализ
- Дифференциальный анализ

Асимметрично

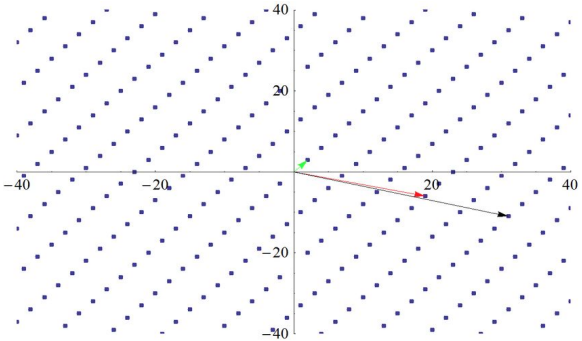
- NP полные задачи(факторизация, дискретный логарифм, решетки)
- В основном арифметика по модулю какого нибудь числа.
- RSA, ECC, diffie-hellman, Paillier, NTRU Prime, CRYSTALS-Kyber, LWE....
- Многоразовые подписи, шифрование, обмен ключами, ZKP, HE и не только

Асимметрично

- Задача факторизации (QFS, NFS, fermat)
- Задача дискретного логарифма (Index, Pohlig-Hellm
- Задача Диффи-Хеллмана
- Задача поиска наименьшего вектора в решетке (LLL)

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

- Side channel и здесь



Тут мы переходим к деталям

Группы

A - набор(множество) каких-либо элементов. Например $A = \{ a_1, a_2, \ldots, a_n \}$

$*$ - бинарная операция: $* : A \times A \to A$. Например $a_1 * a_2 = a_{10}$

$*$ - ассоциативна, если $\forall a, b, c : a * (b * c) = (a * b) * c$

$*$ - коммутативна, если $\forall a, b : a * b = b * c$

$G(*)$:

- $*$ - ассоциативна
- $\forall a, b \in G : a * b \in G.$
- $\exists e \in G : \forall a \in G : a * e = e * a = a$
- $\forall a \in G \exists b : a * b = b * a = e, b = a^{-1}$

Абелева, если $*$ - коммутативна

Примеры

- $\mathbb{Z}(+), \mathbb{Q}(+), \mathbb{R}(+), \mathbb{C}(+), \mathbb{Q} \setminus \{ 0 \} (*)$
- $\mathbb{M}(Z)(+) = M(Z)^{n \times n}(+)$
- $\mathbb{Q}(x)(+) = \{ a_0 + a_1 * x + a_2 * x^2 + \ldots + a_n * x^n | a_i \in \mathbb{Q}, n \in \mathbb{N} \}$
- $\mathbb{M}(\mathbb{R}, \mathbb{R})(+) = \{ f | f : \mathbb{R} \to \mathbb{R} \}$
- $\mathbb{S}(\mathbb{R})(\circ) = \{ f | f : \mathbb{R} \to \mathbb{R}, f - \textit{биективная} \}$

$\mathbb{N}(+)$ - не группа

Модульная арифметика

$a, b \in \mathbb{N}$

$a \geq b$

$a = b * m + r$, r - остаток от деления

$a \equiv r \pmod{b}$

- Рефлексивно. $a \equiv a \pmod{n}$
- Симметрично. $a \equiv b \pmod{n} \implies b \equiv a \pmod{n}$
- Транзитивно. $a \equiv b \pmod{n} \land b \equiv c \pmod{n} \implies a \equiv c \pmod{n}$

$a + b \pmod{n} \equiv a \pmod{n} + b \pmod{n} \pmod{n}$

$a * b \pmod{n} \equiv a \pmod{n} * b \pmod{n} \pmod{n}$

Модульная арифметика

если $gcd(a, b) = d$ то мы можем найти такие числа $k, t : k * a + t * b = d$

$$gcd(a, b) = 1 \implies \exists k, t : k * a + t * b = 1 \implies k * a = 1 - t * b \equiv 1 \pmod{b}$$

$$a * x \equiv b \pmod{n}$$

$$gcd(a, n) = d$$

$$gcd(a, b) = d$$

$$\frac{a}{d} * x \equiv \frac{b}{d} \pmod{\frac{n}{d}}$$

$$x \equiv t \pmod{\frac{n}{d}}$$

$$x = t + r * \frac{n}{d}, r \in [0, d - 1]$$

Китайская теорема об остатках

$$x \equiv a_1 \pmod{p_1}$$

$$x \equiv a_2 \pmod{p_2}$$

- $x = a_1 + K * p_1$
- $a_1 + K * p_1 \equiv a_2 \pmod{p_2}$
- $K \equiv (a_2 - a_1) * p_1^{-1} \pmod{p_2}$
- $K = ((a_2 - a_1) * p_1^{-1})_{p_2} + R * p_2$
- $x = a_1 + ((a_2 - a_1) * p_1^{-1})_{p_2} * p_1 + R * p_1 * p_2$
- $x \equiv a_1 + ((a_2 - a_1) * p_1^{-1})_{p_2} * p_1 \pmod{p_1 * p_2}$

Обобщаем

$$(p_i, p_j) = 1$$

$$x \equiv a_1 \pmod{p_1^{e_1}}$$

$$x \equiv a_2 \pmod{p_2^{e_2}}$$

...

$$x \equiv a_n \pmod{p_n^{e_n}}$$

Конечные группы

Примеры

- $\mathbb{Z}_n(+) = \{\, i | i \geq 0, i < n \,\}$. Модули
- $\mathbb{M}(Z_m)(+) = M(Z_m)^{n \times n}(+)$
- $M_n(Z_m) = \{\, M | M \in M(Z_m)^{n \times n}, det(M) \neq 0 \,\}$
- $\mathbb{Z}_p(*)$

$$GL_n(p), GL_n(Q)$$

$$SL_n = \{\, M | M \in GL_n, det(M) = 1 \,\}$$

- $\mathbb{Z}_{10}(*)$ - не группа
- $\mathbb{M}(Z_m)(*) = M(Z)^{n \times n}(*)$

Подгруппы

$H(*) \leq G(*)$ - подгруппа

- $H \subset G$
- H - группа(замкнута по *)

Критерий: $\forall a, b \in H : a * b^{-1} \in H$

Порядок группы

$|G|$ - количество элементов в группе, порядок группы

- $|Z_n(+)| = n$
- $|Z_p(*)| = p - 1$
- $|GL_n(q)| = (q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1})$
- $|SL_n(q)| = \frac{1}{q-1}|GL_n(F_q)|$
- $|S_n| = n!$

Порядок элемента

$G(*)$ - группа, $g \in G$

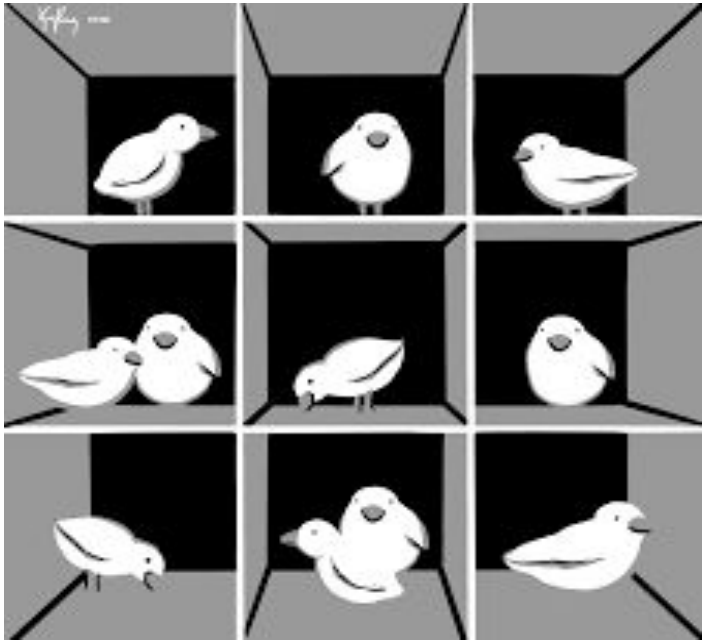
$g^n = g * g * g * g * g \ldots * g$, n раз

$m = ord(g) = min\{ n | n \in \mathbb{N}, g^n = e \}$

$g^{-1} = g^{m-1}$

$g^{q*m+r} = g^r$

$ord(g^k) = \frac{m}{gcd(m,k)}$



Циклические группы

$$G = < g > = \{ g^i | i \in \mathbb{N} \}$$

$$G = < a, b > = \{ a^i * b^j | i, j \in \mathbb{N} \}$$

$$G = < a, b > = \{ a^{i_1} * b^{i_2} * a^{i_3} * \ldots | i_j \in \mathbb{N} \}$$

Теорема Лагранжа

$$\forall g \in G : ord(g) | |G|$$

В циклической:

$$ord(g) = |G|$$

Кольца

$R(+, *)$

- $R(+)-$ Абелева группа
- $R(*)-$ полугруппа.(не у всех элементов есть обратные)
- $*$ (лево)дистрибутивна по $+$: $a * (b + c) = a * b + a * c$

Кольцо с единицей - если есть единица по "умножению"

Коммутативное кольцо - если коммутативно по умножению

ДЕЛИТЕЛИ НУЛЯ

$\exists a, b : a \neq 0, b \neq 0, a * b = 0$

Примеры колец

- $Z_n(+,*)$
- $GL_n(p), SL_n(p)$
- $Z[x], Q[x]$

Поля

$P(+, *)$ - поле

- $P(+, *)$ - коммутативное кольцо с единицей
- у всех элементов кроме нуля есть обратные по умножению

Примеры полей

- $\mathbb{Q}(+, *)$
- $Z_p(+, *)$
- $GF(p^n)(+, *)$

Непосредственно крипта

ДХ

$G(*), g \in G, ord(g) - \textit{большой}$

$A = g^a, B = g^b, C = g^{ab}$

Линии атаки

Атакуем

- BSGS, collision, Pollards
- Pohlig-Hellman
- Man in the middle
- Index
- Какая нибудь обскурная атака из пдфки

RSA

RSA

p, q - большие простые числа

$$n = p * q$$

$$e = 0x10001$$

$$d = e^{-1} \pmod{\phi n}$$

$$c = m^e \pmod{n}$$

$$m = c^d \pmod{n}$$

Почему работает

$$Z_n^* = Z_{p-1} \times Z_{q-1}$$

$$|Z_n^*| = (p-1) * (q-1) = \phi(n)$$

$$e * d = 1 \pmod{\phi n}$$

RSA

Почему сложно

- В общем случае эквивалентно факторизации n

Почему плохо

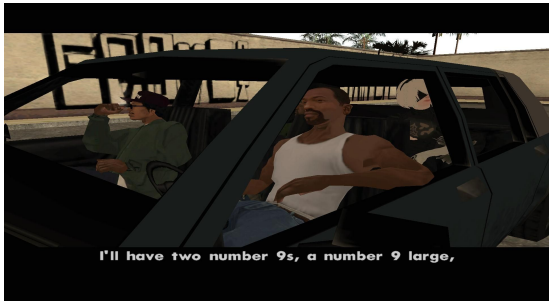
- Для стойкости надо: многа битов, не ошибиться в имплементации(очень сложно)

А как атакуют

RsaCtfTool

Линии атаки

Атакуем

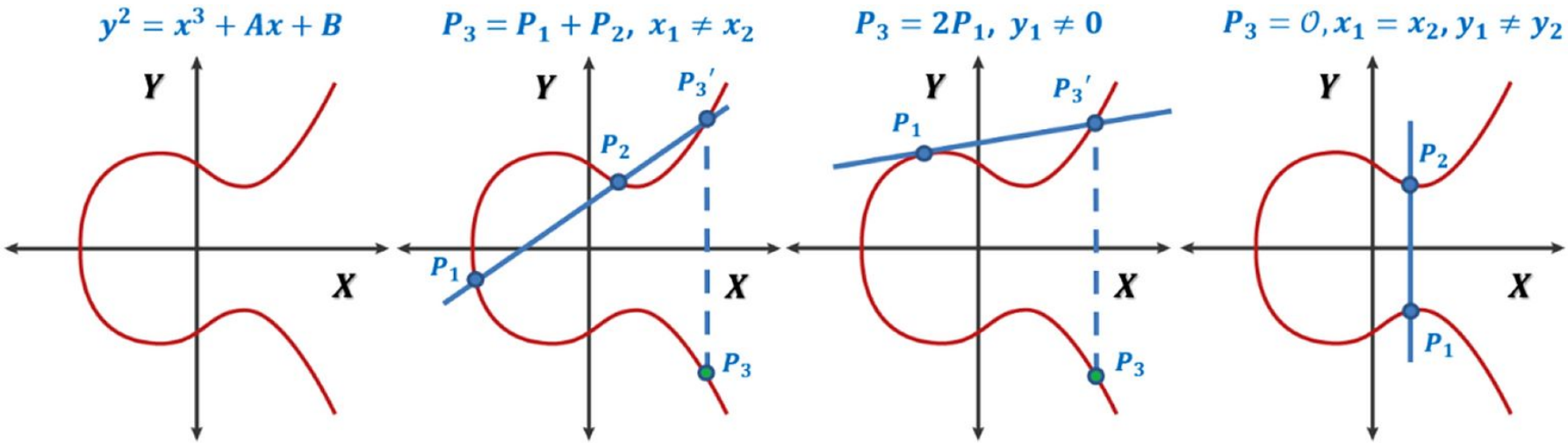


- factor: Fermatt, Pollard, Lenstra, factordb, QFS, NFS, кривой бэкдор, 4p-1, ROCA
- Wiener, Boneh-Durfee, egcd, знаем phi, знаем брутабельную часть d, знаем 0.25 битов d, Cycles
- 3
- PKCS1.5, Don Coppersmith, PARTIAL KEY RECOVERY
- Side channel
- Какая нибудь обскурная атака из пдфки

Эллиптика

$Y^2 = X^3 + A \cdot X + B$ - уравнение эллиптической кривой в форме Вейерштрасса.

$\Delta = -16(4A^3 + 27B^2)$



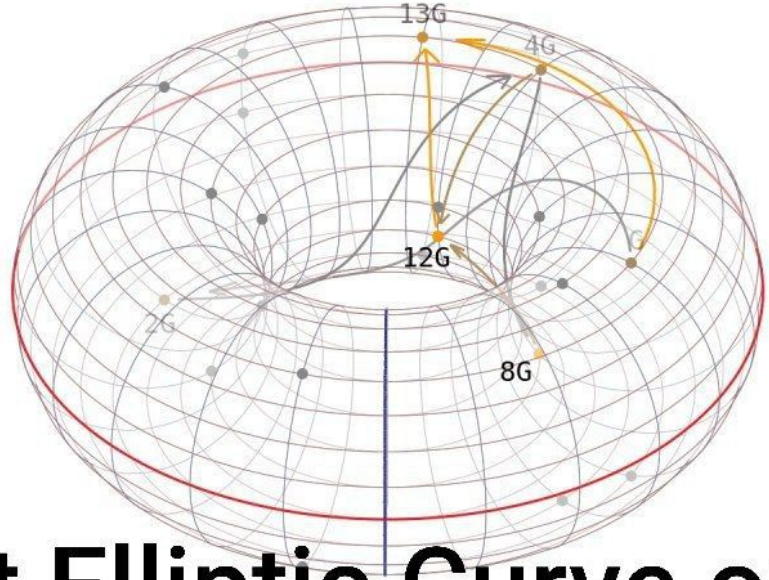
$$P = (x_p, y_p)$$

- $Q = O \Rightarrow P + Q = P$
- $Q = (x_p, -y_p) \Rightarrow P + Q = O$
- $Q \neq P \Rightarrow \lambda = \frac{y_p - y_q}{x_p - x_q}$
- $Q = P \Rightarrow \lambda = \frac{3 * x_p^2 + A}{2 * y_p}$

$$x_r = \lambda^2 - x_p - x_q$$

$$y_r = \lambda(x_p - x_r) - y_p$$

What if we Kissed



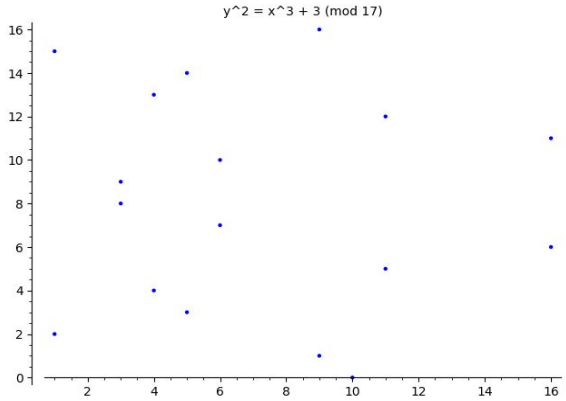
At Elliptic Curve on a torus

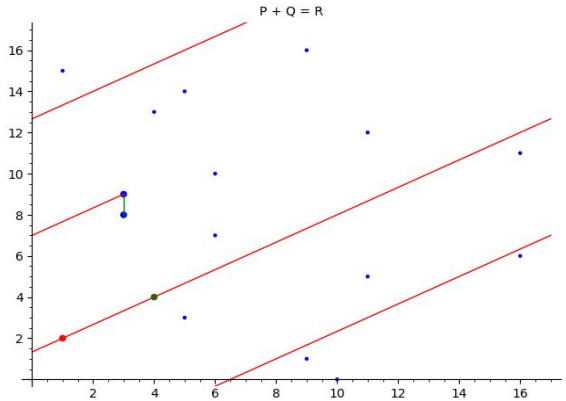
$$E(F_p) = \{ (x, y) | x, y \in F_p, y^2 = x^3 + a * x + b \}$$

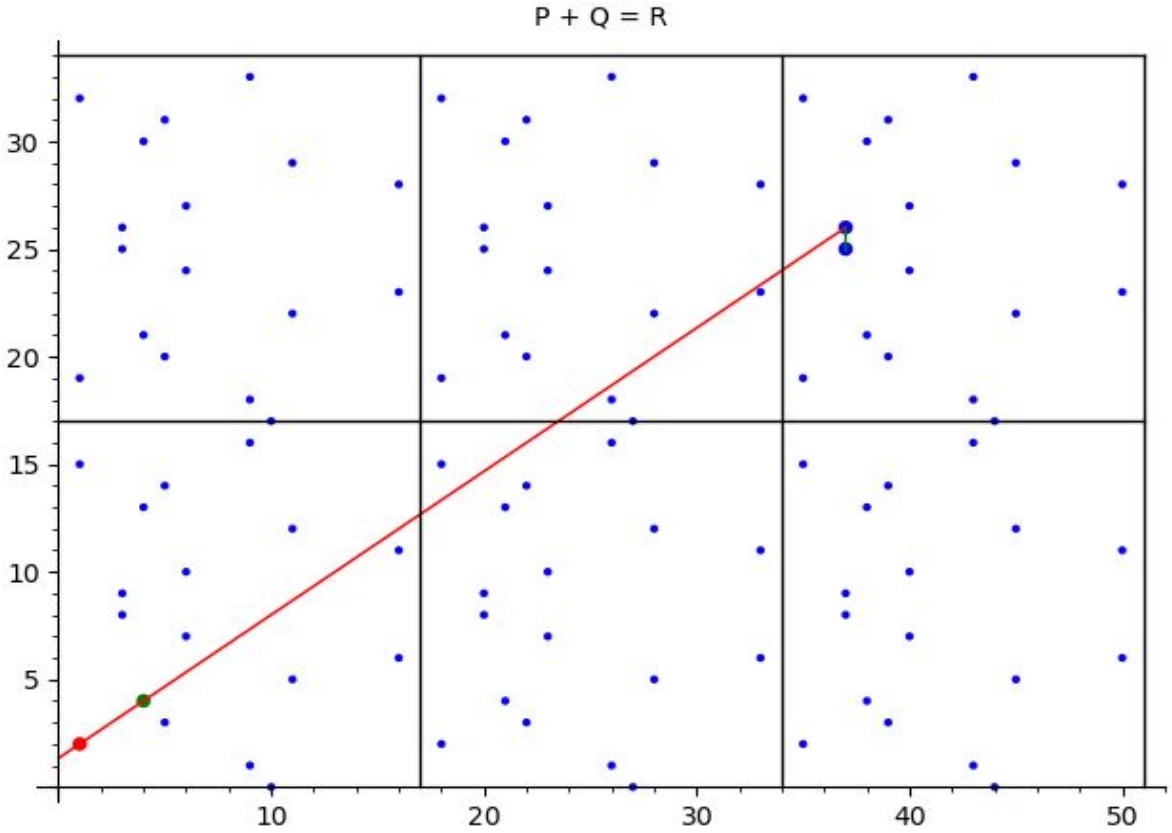
$$|E(F_p)|$$

$$ord(G) = m \iff m * G = O$$

Эллиптические кривые над конечным полем







ДЛП

$$Q = P + P + P + \ldots + P = k * P$$

Задача дискретного логарифма - по заданным P, Q найти k.

$$E(F_p)[r] = = \{ P | P \in E(F_p), r * P = O \}$$

Baby-Step Giant-Step

$n = ord(P) = ord(Q)$

$m = \lfloor \sqrt{n} \rfloor$

$Q = k * P = (i * m + j) * P$

$j * P = Q - i * (m * P)$

Дальше мы заполняем хэш таблицу: $(j * P, j)$ Для того, чтобы иметь хорошие шансы на нахождение коллизии j нужно взять $\in [0, 3\sqrt{n}]$

После этого итерируемся $i \in [0, 3\sqrt{n}]$ и проверяем, есть ли ключ $Q - i * (m * P)$ в таблице.

Атаки на протокол Диффи-Хеллмана

Можно выделить несколько базовых атак на протокол

- Человек посередине.
- Гладкий порядок кривой, точки.
- Недостаточно большой секрет.
- Дискретный логарифм на аномальных кривых.
- Дискретный логарифм на сингулярных кривых.

и не очень

- MOV

ECDSA

- Пара человек соглашается на кривой и точке.
- Алиса на своей стороне выбирает приватный ключ и вычисляет публичный ключ.
- Алиса выполняет следующие действия для подписи сообщения m

$E(F_p)$

G, $ord(G) = q$.

$d_a \in [1, q-1]$. $Q_a = d_a * G$.

1. e = HASH(m)
2. $z = F_p(e)$
3. Случайно выбирается $k \in [1, q-1]$
4. $R = k * G$, $r = R.x$
5. $s = k^{-1} * (z + r * d_a) \pmod{q}$
6. (r, s) - цифровая подпись сообщения m.

ECDSA

- Проверка подписи

1. $u_1 = z * s^{-1} \pmod{q}$
2. $u_2 = r * s^{-1} \pmod{q}$
3. $(u_1 * G + u_2 * Q_a).x == r$

- Корректность проверки

$$u1 * G + u2 * Q_a = z * s^{-1} * G + r * s^{-1} * Q_a = s^{-1} * (z * G + r * d_a * G) = s^{-1} * (z + r * d_a) * G =$$

$$= s^{-1} * s * k * G = k * G$$

Атаки на ECDSA

Можно выделить несколько базовых атак на алгоритм

- Повторное использование nonce.
- Использование LCG и NLCG при генерации nonce.
- Атака на ECDSA с использованием LLL алгоритма.

Безопасные кривые

- https://safecurves.cr.yp.to/

X Функции

Хеш функции

- Быстро считается, сложно обращается(почти одностороннее отображение)
- Почти односторонние отображения, но не такие как в шифровании

- sha1, sha2, sha3, md, блейк, шейк и две дымящихся шашки

- Целостность сообщений, электронные подписи, пароли с солью.

Хэш функции

- Стойкость к поиску прообраза (preimage resistance)
- Стойкость к поиску второго прообраза(second preimage resistance)
- Стойкость к коллизиям(collision resistance)

$$x? : H(x) = h$$

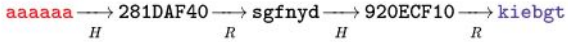
$$x? : H(y) = H(x)$$

$$x, y? : H(x) = H(y)$$

А как, а зачем

Атакуем

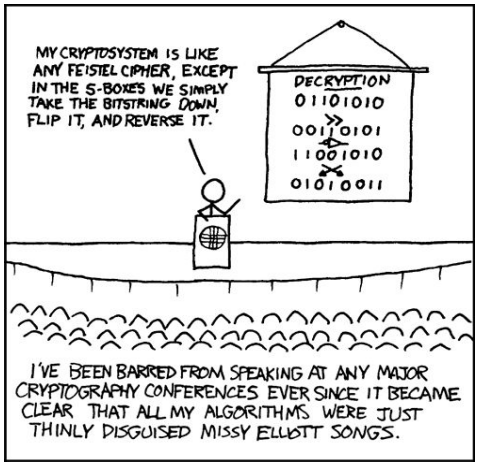
- Парадокс дней рождений
- Возвращение полларда
- Meet in the middle
- Дифференциальный криптоанализ
- Радужные таблицы



hash	year	coll. res.	size (bits)	design	broken?
MD4	1990	64	128	32-bit ARX DM	1995
SHA-0 (SHA)	1993	80	160	32-bit ARX DM	1998
MD5	1993	64	128	32-bit ARX DM	2004
SHA-1	1995	80	160	32-bit ARX DM	2005
SHA-256 (SHA-2)	2002	128	256	32-bit ARX DM	
SHA-384 (SHA-2)	2002	192	384	64-bit ARX DM	
SHA-512 (SHA-2)	2002	256	512	64-bit ARX DM	
SHA-224 (SHA-2)	2008	112	224	32-bit ARX DM	
SHA-512/224	2012	112	224	64-bit ARX DM	
SHA-512/256	2012	128	256	64-bit ARX DM	
SHA3-224	2013	112	224	64-bit Keccak sponge	
SHA3-256	2013	128	256	64-bit Keccak sponge	
SHA3-384	2013	192	384	64-bit Keccak sponge	
SHA3-512	2013	256	512	64-bit Keccak sponge	
SHAKE128	2013	$\leq$128	any	64-bit Keccak sponge	
SHAKE256	2013	$\leq$256	any	64-bit Keccak sponge	

Симметричное шифрование

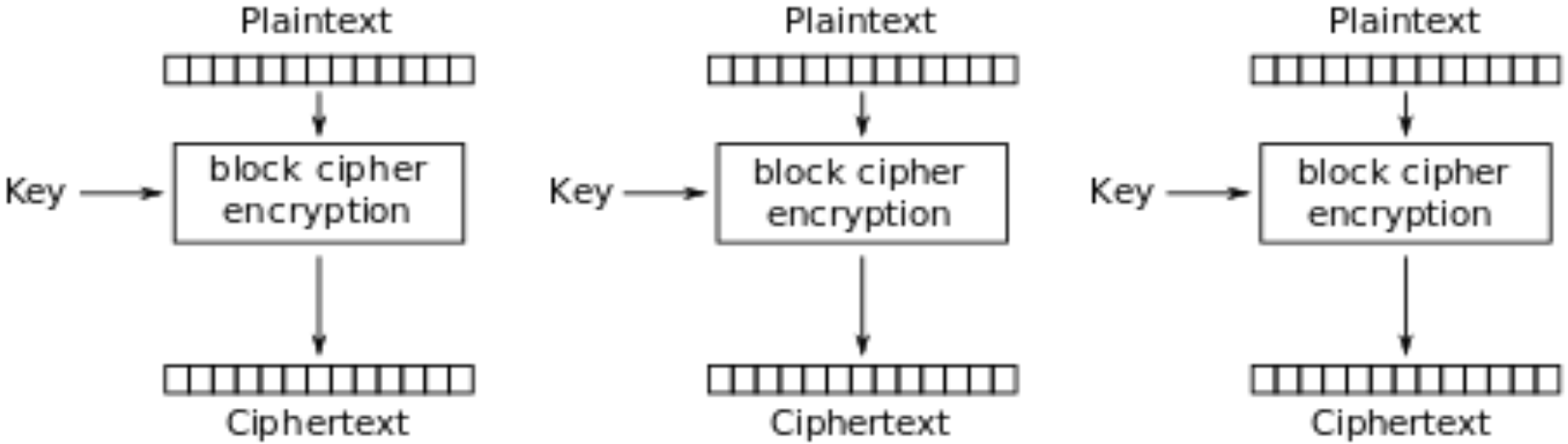
- Булевы функции, S-boxы и много-много битов
- Цезарь, Виженер, OTP, AES, DES, ChaCha20, RC4, Feistel...
- Очевидно однозначные отображения



Блочные шифры

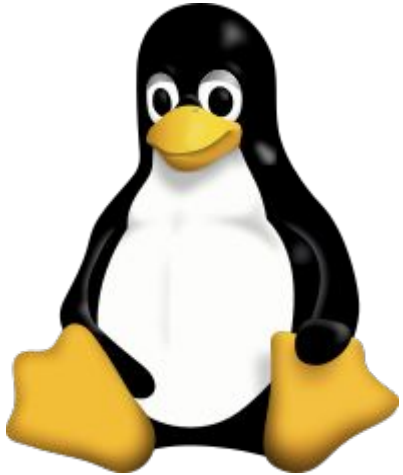
- AES, DES, Feistel, Кузнечик, ГОСТ 28147-89

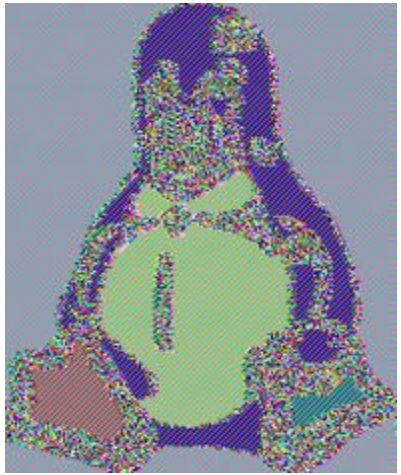
ECB



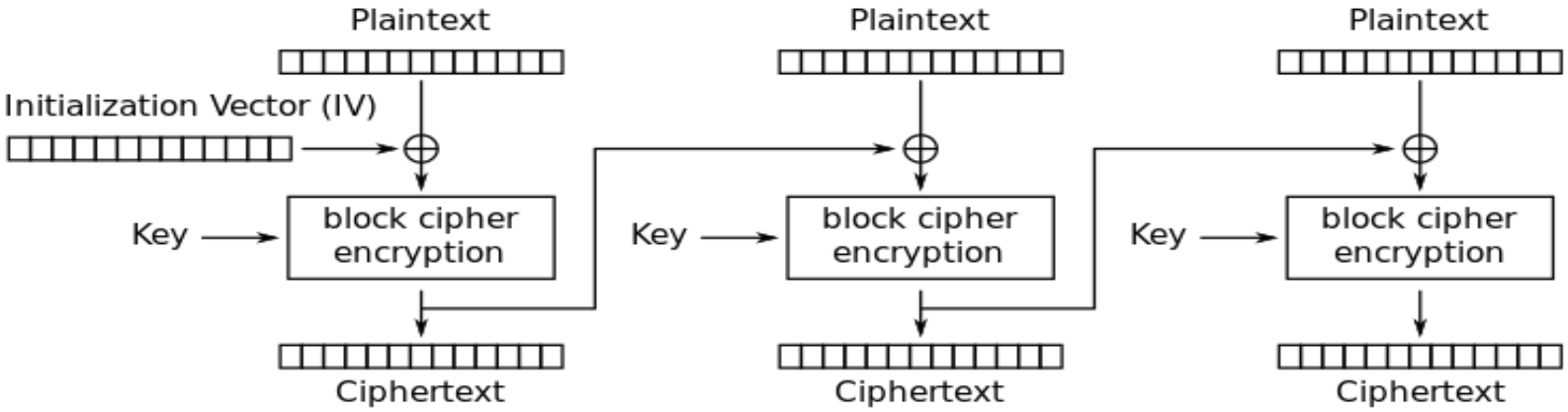
Electronic Codebook (ECB) mode encryption

ECB



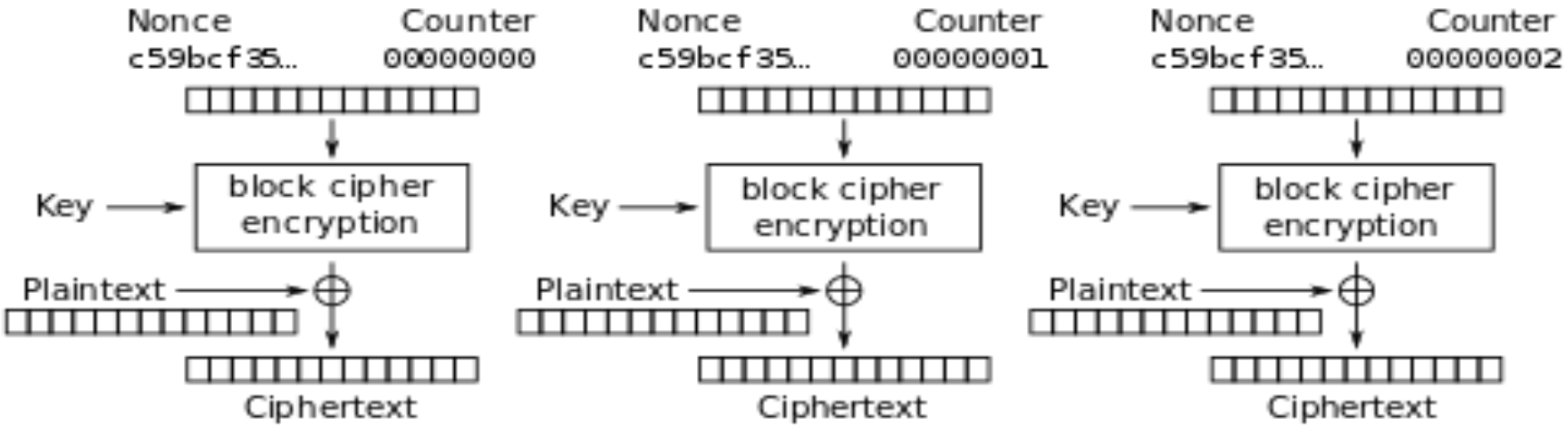


CBC



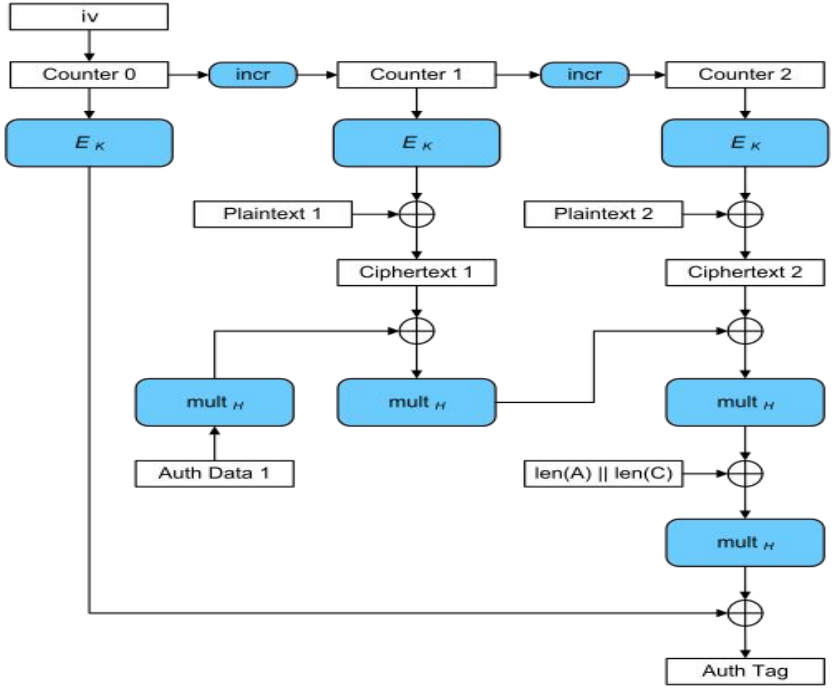
Cipher Block Chaining (CBC) mode encryption

CTR



Counter (CTR) mode encryption

GCM


iv
Counter 0
incr
Counter 1
incr
Counter 2
E K
E K
E K
Plaintext 1
Plaintext 2
Ciphertext 1
Ciphertext 2
mult H
mult H
mult H
Auth Data 1
len(A) || len(C)
mult H
Auth Tag

Атаки на блочные шифры

Атакуем

- Кривые руки программистов
- Meet in the middle
- Дифференциальный криптоанализ
- Линейный криптоанализ
- Слайды
- Biclique attack
- Алгебраические атаки

An Introduction to Mathematical Cryptography (2014) - Hoffstein, Pipher, Silverman.pdf

A graduate course in applied cryptography https://toc.cryptobook.us/

Места, в которых вы будете чаще всего во время цтфа

- https://iacr.org/ Wikipedia
- https://www.springer.com/gp
- https://ru.wikipedia.org
- Какой-нибудь http сайт из 2005
- Сайт со сканами бумаг из 1984
- https://pycryptodome.readthedocs.io/en/latest/

Тренироваться

- https://cryptohack.org/
- https://cryptopals.com/
- https://picoctf.org/
- https://www.sagemath.org/
- https://cr.yp.toc.tf/

Доп материалы 2

- http://factordb.com/
- https://github.com/RsaCtfTool/RsaCtfTool
- https://cryptii.com/
- https://github.com/hellman/xortool
- https://github.com/bbuhrow/yafu
- https://cado-nfs.gitlabpages.inria.fr/

Доп материалы 3

- http://factordb.com/
- https://github.com/RsaCtfTool/RsaCtfTool
- https://github.com/bbuhrow/yafu
- https://cado-nfs.gitlabpages.inria.fr/

- Twenty years of attacks on the RSA
- Recovering cryptographic keys from partial information, by example

- https://github.com/Sarkoxed/MEPhI-CTF-Lectures

Доп материалы 5

1. https://en.wikipedia.org/wiki/Elliptic_curve - База
2. https://www.garykessler.net/library/crypto.html#ecc – еще база
3. https://toc.cryptobook.us/book.pdf - книга по криптографии в целом с хорошим вводом в ECC
4. https://www.math.auckland.ac.nz/~sgal018/crypto-book/main.pdf - книга по криптографии в целом с хорошим вводом в ECC(2)
5. https://crypto.stanford.edu/pbc/notes/ep/curve.html - если вам легче изучать программируя
6. https://people.cs.nctu.edu.tw/~rjchen/ECC2012S/Elliptic%20Curves%20Number%20Theory%20And%20Cryptography%202n.pdf – результат нескольких веков изучения кривых