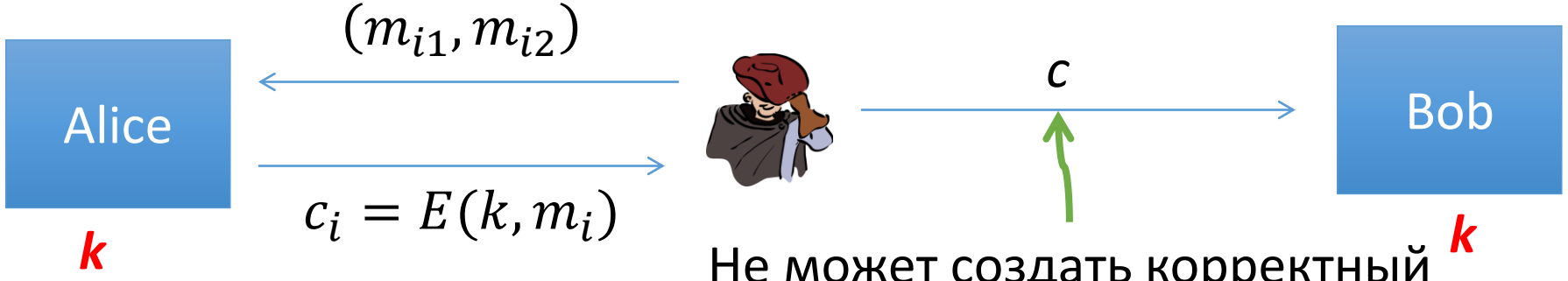
Асимметричная криптография

Макаров Артём

МИФИ 2020

Аутентифицированное шифрование

- Предполагается наличие **общего секретного ключа**
- Пассивный противник не может расшифровать сообщения
- Активный противник не может вставлять или изменять сообщения в канале
- Целостность шифртекстов обеспечивает целостность открытых текстов



Не может создать корректный $c \notin \{ c_1, \ldots, c_q \}$

Не может различить зашифрования m_{i1}, m_{i2}

Не может расшифровать c_i

Согласование ключей

- Генерация одной из сторон и передача другой (обмен ключей)
- Генерация доверенной третьей стороной
- Выработка ключа из общего ключевого материала

Необходимо обеспечение целостности и секретности согласованных ключей.

Согласование ключей

Все описанные способы согласования ключей можно реализовать средствами симметричной криптографии, но при условии наличия общего симметричного ключа. Т.е. для получения общего секретного ключа необходим уже существующий общий секретный ключ.

Хотелось бы иметь возможность согласования ключей, без необходимости иметь общий секретный ключ со всеми участниками.

Асимметричная криптография

- Использование двух различный ключей – открытого ключа PK (public key) и закрытого ключа SK (secret key)
- Предполагается секретность только закрытого ключа, открытый ключ общеизвестен
- Открытый ключ используется для шифрования и проверки подписи, закрытый для расшифрования и подписания
- Операции шифрования и расшифрования, подписи и проверки различны (т.е. преобразования асимметричны)
- В общем случае намного медленнее симметричных криптосистем

Протокол обмена ключей Diffie-Hellman’a

Пусть имеется незащищенный открытый канал связи при условии пассивного противника.

Хотим получить возможность согласования общего ключа для Алисы и Боба.

Пассивное прослушивание

Кратко о мультипликативной группе

- Пусть p простое число. Пусть Z_p^* - циклическая мультипликативная группа по модулю p, $\left|Z_p^*\right| = \phi(p) = p - 1$.
- $\forall x \in Z_p^*. x^{p-1} = 1, 1$ – единичный элемент в группе Z_p^*
- Пусть $g \in Z_p^*$ - генератор, т.е. $< g > = Z_p^*$.
- $\forall x \in Z_p^* \exists n: x = g^n$

Пример. Пусть $p = 7$.

$Z_7^* = \{3, 2, 6, 4, 5, 1\}$, $g = 3$

Протокол обмена ключей Diffie-Hellman’a

Пусть p большое простое число: $\frac{p-1}{2}$ - простое.

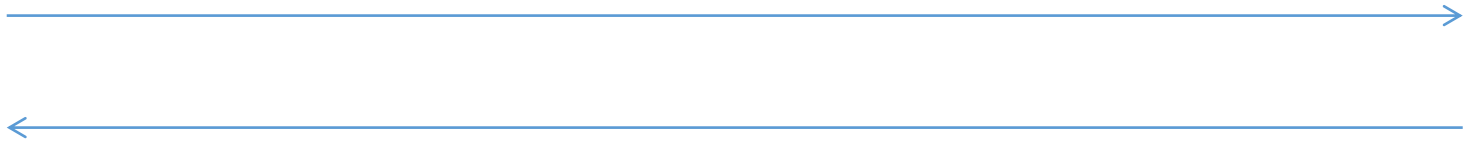
Пусть g – генератор в Z_p^*

Alice

choose random **a** in {1,…,p-1}

Bob

choose random **b** in {1,…,p-1}



$\mathbf{B^a} \pmod p = (g^b)^a = \mathbf{k_{AB} = g^{ab}} \pmod p = (g^a)^b = \mathbf{A^b} \pmod p$

NB: для формирования итогового симметричного ключа используют хэш от итогового значения k_{ab}, или другие техники выработки ключа из ключевого материала.

Стойкость

Противник видит $p, g, A = g^a (mod\ p), B = g^b (mod\ p)$

Противник хочет вычислить $g^{ab} (mod\ p)$

Пусть $DH_g\left(g^a, g^b\right) = g^{ab}$. Насколько сложно вычисление DH?

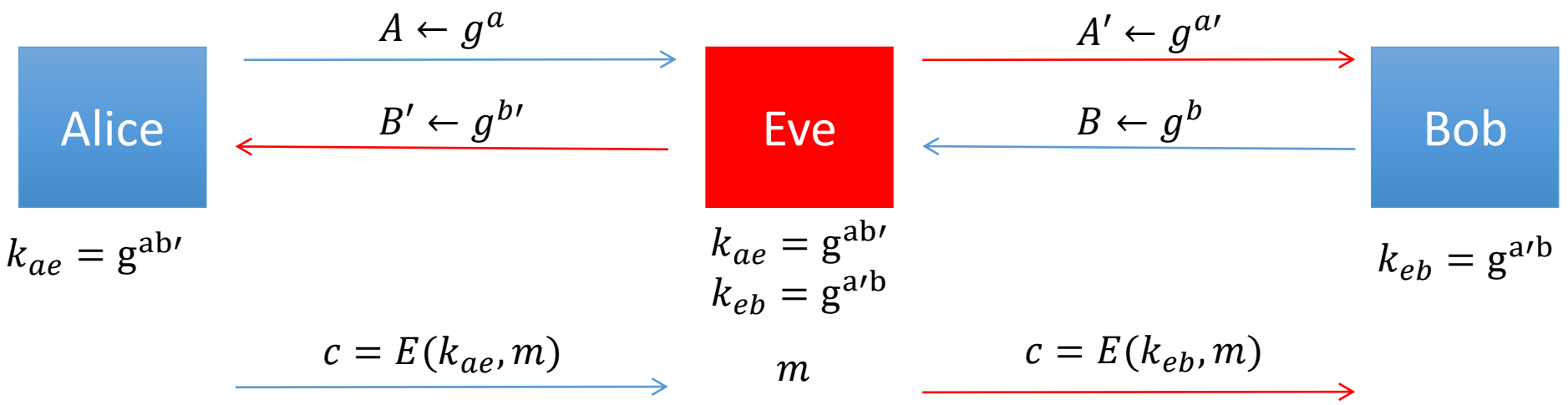
$T(DH) = \exp(O(n^{\frac{1}{3}}))$.

cipher key size	modulus size	Elliptic Curve size
80 bits	1024 bits	160 bits
128 bits	3072 bits	256 bits
256 bits (AES)	**15360** bits	512 bits

As a result: slow transition away from (mod p) to elliptic curves

Отсутствие стойкости против активных противников

- Протокол не гарантирует аутентичности, т.е. вы не знаете, с кем согласовали ключ.
- Возможны атаки типа человек в середине (MiTM – man in the middle)



Асимметричное шифрование (шифрование с открытым ключом)

Пусть $\mathrm{E} = (G, E, D)$ на $(\mathrm{PK}, \mathrm{SK}, X, Y), k$ – параметр:

- $G: 1^k \to_r (SK, PK): (SK, PK) \in (\mathrm{PK} \times \mathrm{SK})$ – генерация ключей
- $E: \mathrm{PK} \times X \to_r Y$ – зашифрование
- $D: \mathrm{SK} \times Y \to X$ – расшифрование

E – эффективно вычислим, выполняется свойство корректности.

Для простоты примем E – стойким, если противник, имея шифртекст и открытый ключ, а также пары открытый текст-шифртекст не может восстановить искомый открытый текст.

RSA (упрощённо)

G:

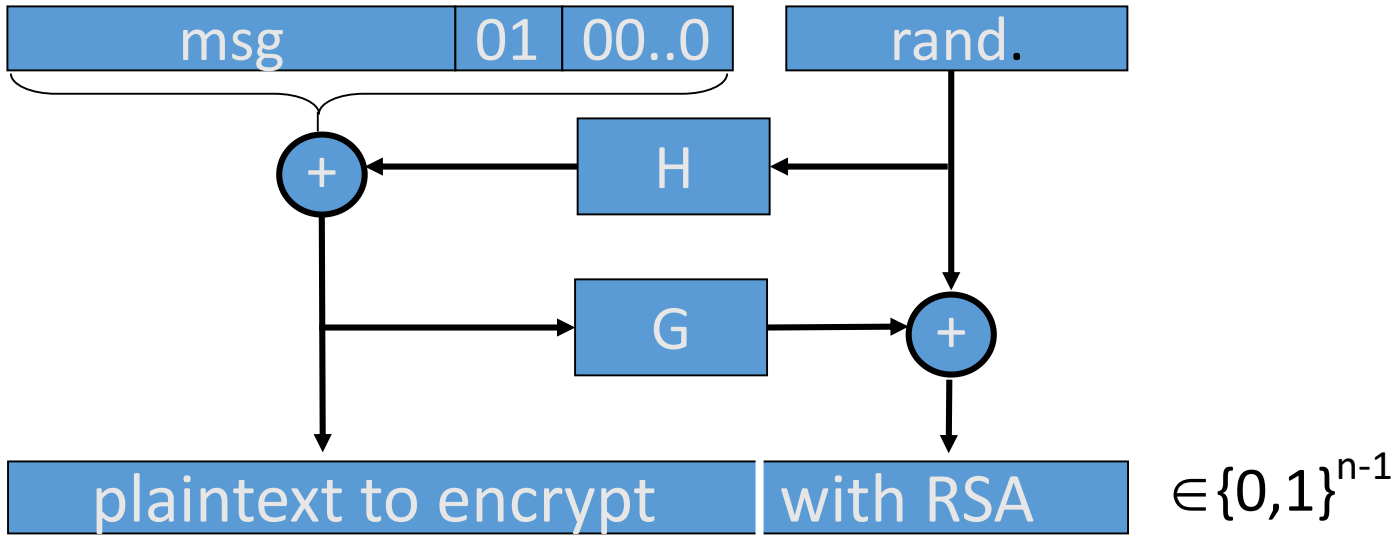
- выбрать 2 больших простых числа $p, q. N = pq$
- Выбрать числа $e, d: ed = 1(mod\ \phi(N))$
- $PK = (N, e), sk = (N, d)$

E_{PK}: $Z_N^* \to Z_N^* : E(x) = x^e mod\ N.$	D_{SK}: $Z_N^* \to Z_N^*: D(y) = y^d = x^{ed} =$ $x^{ed(mod\ \phi(N))} =$ $x^{k*\phi(N)+1\ (mod\ \phi(N))} = x$.

PKCS1 v2.0: OAEP

Режим для шифрования RSA: OAEP (Optimal Asymmetric Encryption Padding)

Проверка дополнения
при расшифровании.
Отклонение,
при несовпадении.



Thm [FOPS'01] : RSA is a trap-door permutation $\Rightarrow$
RSA-OAEP is CCA secure when H,G are *random oracles*

На практике: использование SHA-256 для H и G

Криптосистема Эль-Гамаля (упрощённо)

G – циклическая группа порядка n (например Z_p^*)

(E_S, D_s) - симметричный аутентифицированный шифр на (K, M, C)

$H: G^2 \to K$ – хэш-функция.

$\boldsymbol{G}: g \leftarrow^R$ Генарторы $G; a \leftarrow Z_n; SK = a, pk = (g, h = g^a)$

$\boldsymbol{E}(\boldsymbol{PK} = (\boldsymbol{g}, \boldsymbol{h}), \boldsymbol{m})$:	$\boldsymbol{D}\big(\boldsymbol{sk} = \boldsymbol{a}, (\boldsymbol{u}, \boldsymbol{c})\big)$:
$b \leftarrow^R Z_n, u \leftarrow g^b, v \leftarrow h^b$ $k \leftarrow H(u, v), c = E_s(k, m)$ $C = (u, c)$	$v \leftarrow u^a$ $k \leftarrow H(u, v), m = D_s(k, c)$

Электронные подписи

Пусть $\mathrm{D} = (G, S, \mathrm{V})$ на $(\mathrm{PK}, \mathrm{SK}, X, \Sigma), k$ – параметр:

- $G: 1^k \to_r (SK, PK): (SK, PK) \in (\mathrm{PK} \times \mathrm{SK})$ – генерация ключей
- $S: \mathrm{SK} \times X \to \sigma$ – подписание, $\sigma \in \Sigma$
- $V: \mathrm{PK} \times X \times \sigma \to_r \{0,1\}$ – проверка подписи

D – эффективно вычислим, выполняется свойство корректности.

Для простоты примем D – стойким, если противник, имея пары сообщение-подпись не может сформировать новую подпись.

Подпись на основе RSA (упрощённо)

G:

- выбрать 2 больших простых числа p, q. $N = pq$
- Выбрать числа e, d: $ed = 1(mod\ \phi(n))$
- $PK = (N, e), SK = (N, d)$

$S_{PK}: Z_N^* \to Z_N^* : S(x) = x^d mod\ N.$	$V_{SK}: Z_N^* \to Z_N^*: V(y) = y^e =? x;$ $y^e = x^{ed} = x^{ed(mod\ \phi(N))} =$ $x^{k*\phi(N)+1\ (mod\ \phi(N))} = x$.

DSA (упрощённо)

G – циклическая группа порядка q (например Z_p^*)

$H: G^2 \to K$ – хэш-функция

$\boldsymbol{G}: g \leftarrow^R$ Генарторы $G; a \leftarrow Z_n; SK = a, pk = (g, h = g^a)$

$\boldsymbol{S}(\boldsymbol{SK} = \boldsymbol{a}, \boldsymbol{m})$:	$\boldsymbol{V}(\boldsymbol{PK} = (\boldsymbol{g}, \boldsymbol{h} = \boldsymbol{g}^{\boldsymbol{a}}, \boldsymbol{m}, \boldsymbol{\sigma})$:
$k \leftarrow^R \{1..q-1\}$	$w = s^{-1} \bmod q$
$r \leftarrow g^k \bmod \text{p} \pmod \text{q}$	$u_1 = H(m)w \bmod q$
$s = k^{-1}(H(m) + ar)) \pmod \text{q}$	$u_2 = rw \bmod q$
$\sigma = (r, s) \pmod \text{q}$	$v = (g^{u_1} h^{u_2} \, mod \, p) \bmod q$
	$v =? r$

Стойкость RSA и Эль-Гамаля

- Стойкость Эль-Гамаля сводится к стойкости одного из предположений о стойкости Диффи-Хеллмана (Hash-DH), которая может быть сведена к задаче нахождения дискретного логарифма.

- Стойкость RSA сводится к сложности задачи нахождения дискретного логарифма, которая сводится к задаче факторизации больших целых чисел.

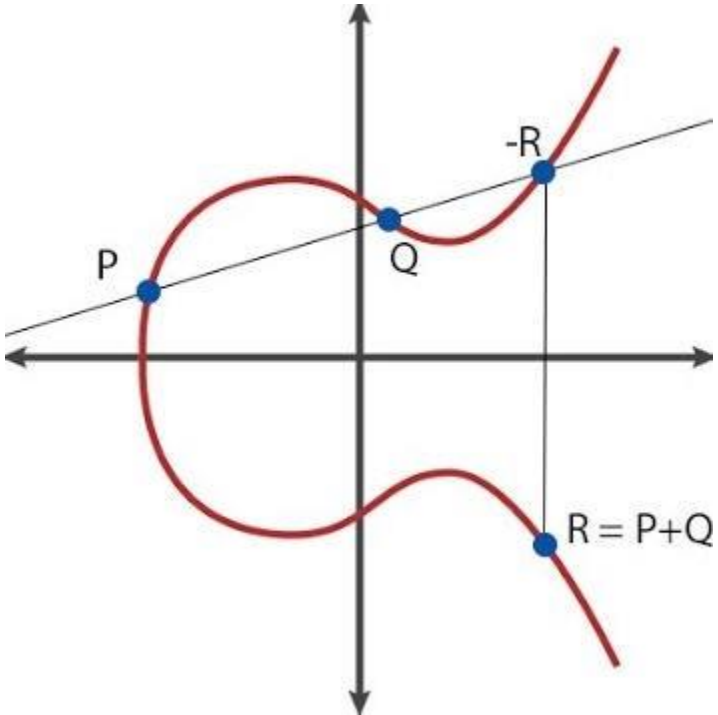
Группа точек эллиптических кривых

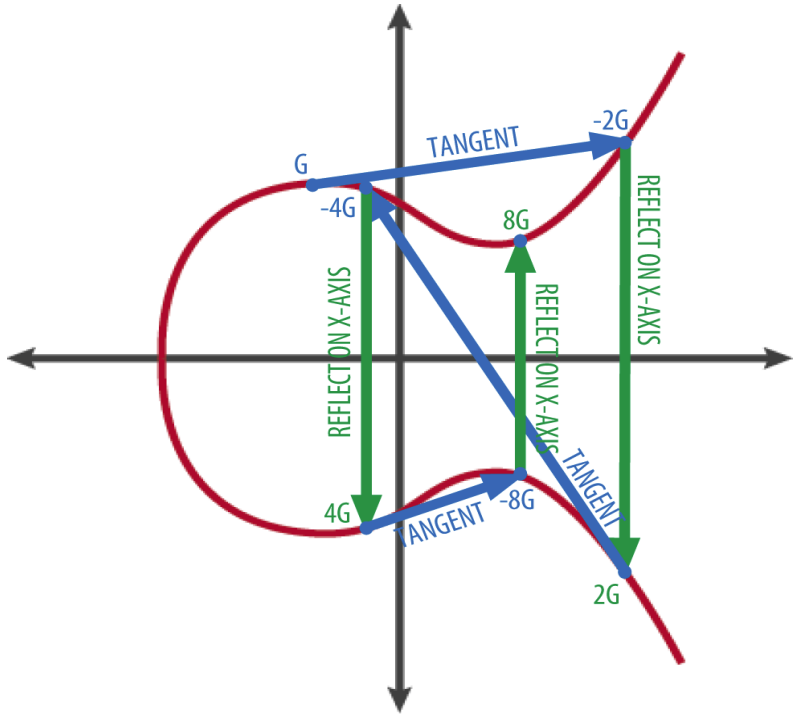
Минус мультипликативных циклических групп – большой размер параметров, при которых криптосистемы на их основе становятся стойкими. Как следствие – большой размер ключей, подписей, шифртекстов.

Если ли группы, элементы в которых имеют меньший размер, но для которых выполняется предположение о сложности нахождения дискретного логарифма и решении задач Диффи-Хеллмана?

Группа точек эллиптических кривых

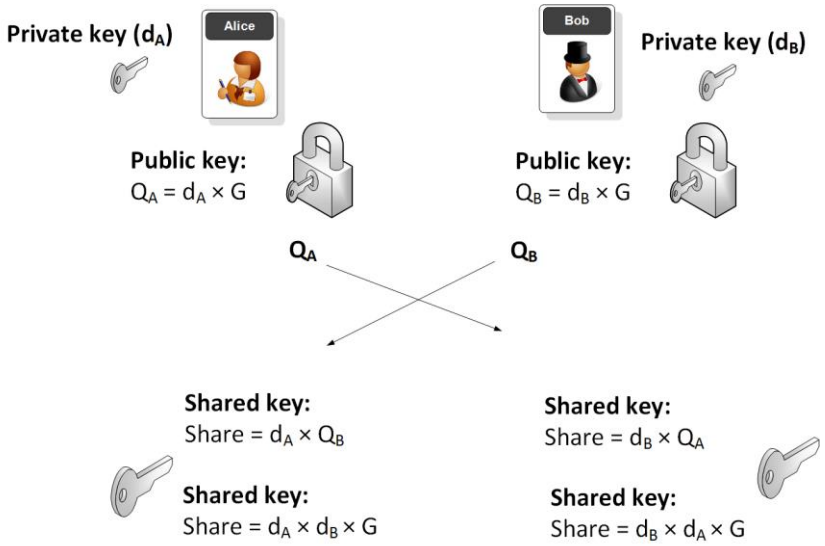
Группа точек эллиптической кривой – группа точек, образованная целочисленными точками на некоторой эллиптической кривой с введённой операцией умножения точки G на число n, определяемой как $nG = \underbrace{G + \cdots + G}_{n}$





Группа точек эллиптических кривых

Можем ввести аналоги протоколов Дифии-Хеллмана и DSA, путём замены групп и замены операций возведения в степень на операцию умножения точки на число.



Для фиксированных кривых в группе точек задачи нахождения дискретного логарифма и задачи Диффи-Хеллмана трудные.