Ассиметричные криптосистемы

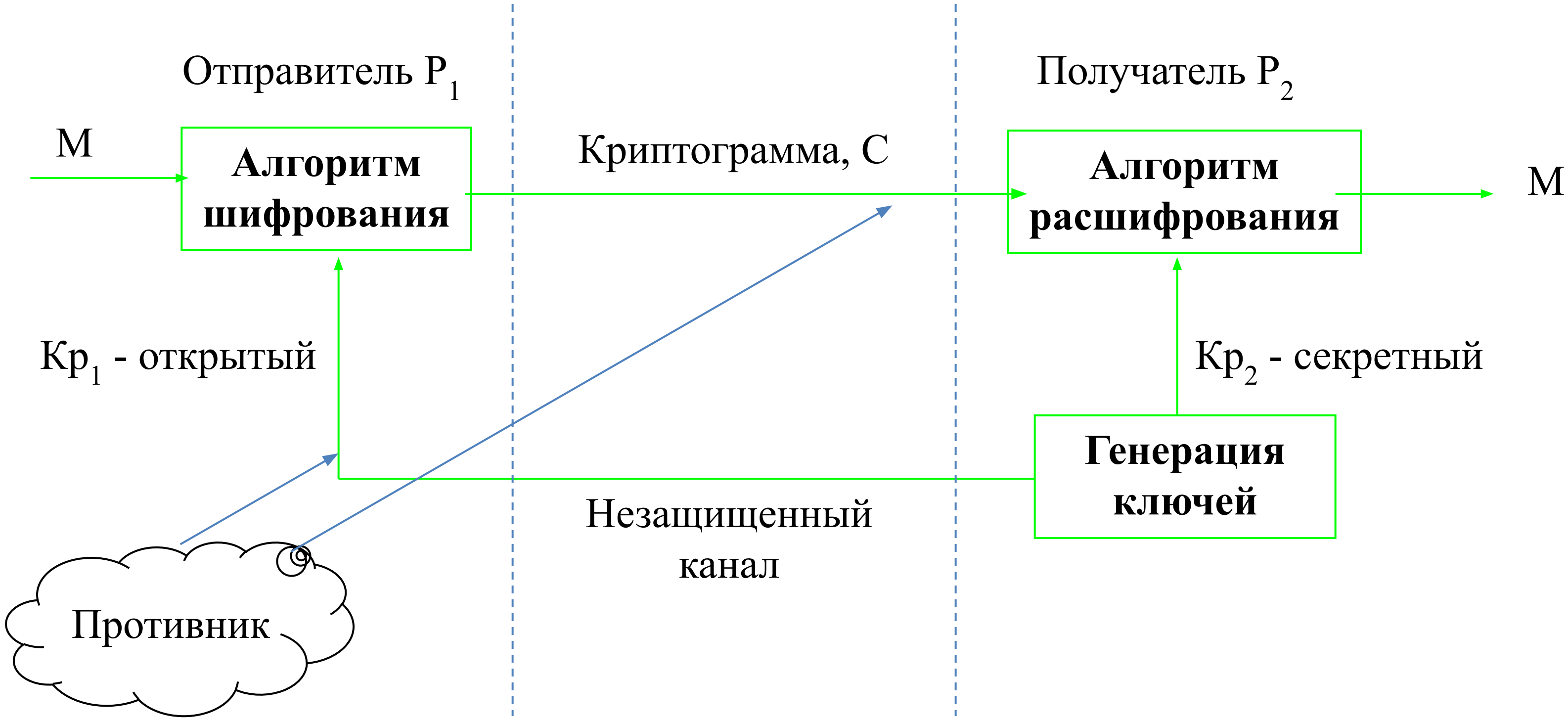
Огюст Керкгоффс

В 80-х годах XIX века издал книгу *"Военная криптография"* объемом всего в 64 страницы, но они обессмертили его имя в истории криптографии.

Керкгоффс сформулировал общие требования к шифрам:

- **простота практического использования;**
- **надежность;**
- **операции шифрования и расшифрования не должны требовать значительных затрат времени.**

Обобщенная схема асимметричной криптосистемы с открытым ключом



Алгоритм Диффи – Хеллмана
(Diffie - Hellman)

Отправитель P_1 **Получатель P_2**

открытые

1. <u>Генерация</u> n, a

модуль основание

2. Случайное число X, вычисляет $A = a^x \pmod n$

A

3. Случайное число Y, вычисляет $B = a^y \pmod n$

4. <u>Вычисление ключа</u> $Kp_1 = B^x \pmod n$

B

5. <u>Вычисление ключа</u> $Kp_2 = A^y \pmod n$

Пример

$n = 5, a = 7, x = 3, y = 2$

$A = 7^3 \pmod 5 = 343 \pmod 5 = 3$

$Kp_1 = 4^3 \pmod 5 = 64 \pmod 5 = 4$

$B = 7^2 \pmod 5 = 49 \pmod 5 = 4$

$Kp_2 = 3^2 \pmod 5 = 4$

Алгоритм RSA (Rivest-Shamir-Adleman)

Генерация ключей

Получатель 1. P, Q - простые, $N = P \cdot Q$

2. $\varphi(N) = (P-1) \cdot (Q-1)$, $\varphi(N)$ - функция Эйлера

Выбор открытого ключа Y:

$1 < Y \leq \varphi(N)$, НОД$(Y, \varphi(N)) = 1$

Вычисление секретного ключа X:

$X \cdot Y \equiv 1 \pmod{\varphi(N)}$ (N,Y) → отправителю

Отправитель шифрование M ($M_i = 0, 1, 2, \ldots, N-1$)

3. $C_i = M_i^Y \pmod N$

Получатель расшифрование $C(C_1, C_2, \ldots, C_i, \ldots)$

4. $M_i = C_i^X \pmod N$

Пример

Генерация ключей

1. $P = 3$, $Q = 11$, $N = P \cdot Q = 33$

2. $\varphi(N) = (P-1) \cdot (Q-1) = 2 \cdot 10 = 20$

$Y = 7$, НОД$(Y, \varphi(N)) = 1$

$X \cdot Y = 1 \pmod{20}$, $7 \cdot 3 = 1 \pmod{20}$, $X = 3$

Сообщение: $M_1M_2 \to 32$; $M_1 = 3 < 33$, $M_2 = 2 < 33$

Шифрование $C_i = M_i^Y \pmod N$

3. $C_1 = 3^7 \bmod 33 = 2187 \bmod 33 = 9$

$C_2 = 2^7 \bmod 33 = 128 \bmod 33 = 29$ Шифротекст 9,29

Расшифрование $M_i = C_i^X \pmod N$

4. $M_1 = 9^3 \bmod 33 = 729 \bmod 33 = 3$

$M_2 = 29^3 \bmod 33 = 24389 \bmod 33 = 2$ Восстановленный текст 3,2

Алгоритм Эль-Гамаля (El Gamal)

<u>Генерация ключей</u>

1. P, G - простые (P>G)
2. X - секретный ключ, (случайное целое X<P)
3. Y - открытый ключ $Y = G^X \bmod P$

<u>Шифрование M</u>

4. К - случайное целое, 1<К<(P-1), НОД(К, P-1) = 1

$a = G^K \bmod P$ $b = Y^K M \bmod P$ (a, b) - шифротекст

<u>Расшифрование (a, b)</u>

5. $M = (b / a^X) \bmod P$

Пример

<u>Шифрование M = 5</u>

1. P = 11, G = 2 (P>G)
2. X<P, X = 8 - секретный ключ
3. $Y = G^X \bmod P = 2^8 \bmod 11 = 256 \bmod 11 = 3$

   Y = 3 - открытый ключ
4. К = 9, НОД(К, P-1) = 1, НОД(9, 10) = 1

   $a = G^K \bmod P = 2^9 \bmod 11 = 512 \bmod 11 = 6$

   $b = Y^K M \bmod P = 3^9 \cdot 5 \bmod 11 = 19683 \cdot 5 \bmod 11 = 9$

   <u>(a, b) = (6, 9) - шифротекст</u>

<u>Расшифрование</u>

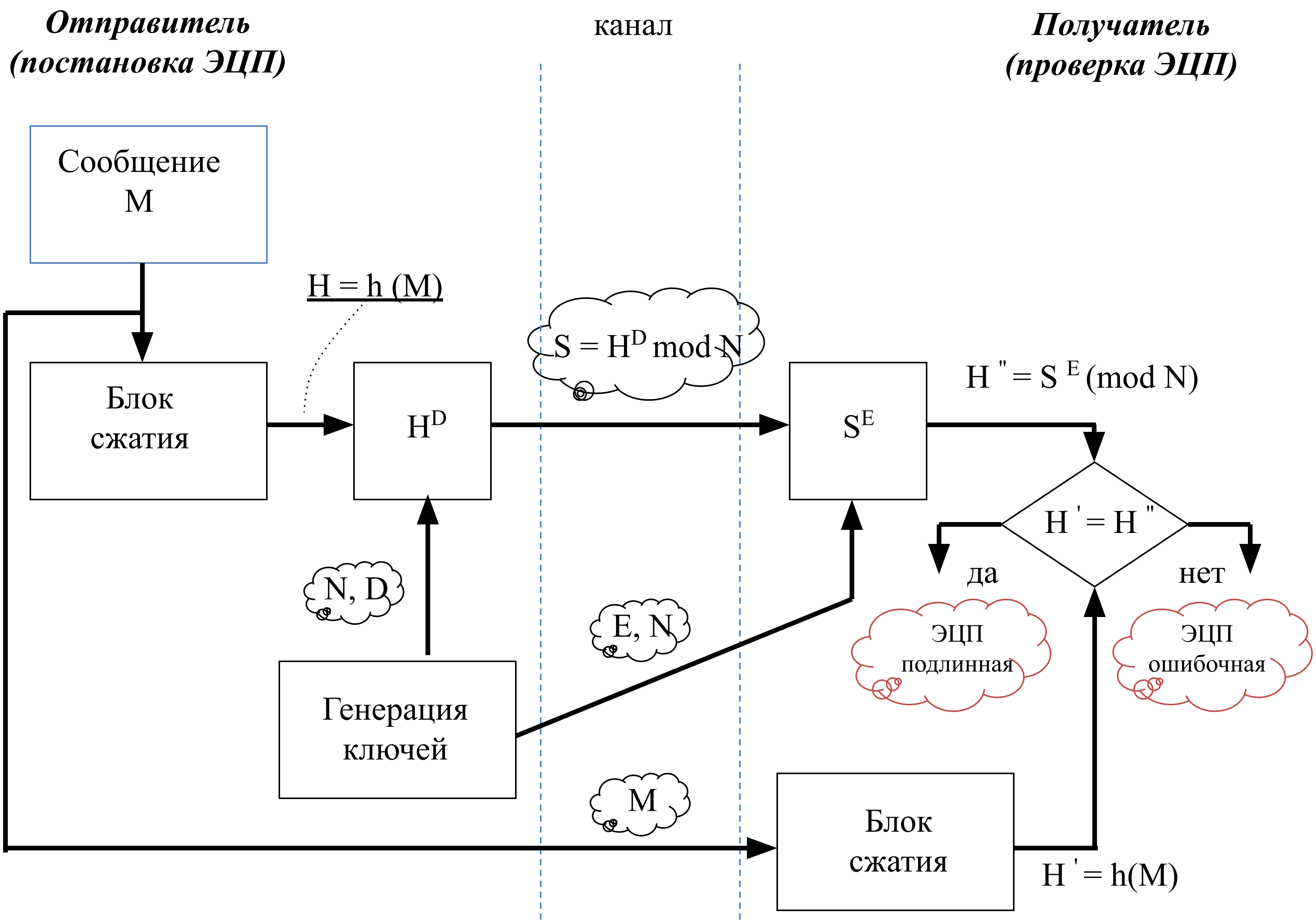
5. $M = (b / a^X) \bmod P = 9 / 6^8 \bmod 11$

   $6^8 M = 9 \bmod 11$

   $1679619 \cdot M = 9 \bmod 11$

   <u>M = 5</u>

Обобщенная схема формирования ЭЦП



ЭЦП RSA

<u>Генерация ключей</u>

1. P, Q - большие простые числа.
2. Модуль $N = P \cdot Q$; $\varphi(N) = (P-1) \cdot (Q-1)$, $\varphi(N)$ - функция Эйлера
3. Открытый ключ $E \le \varphi(N)$; НОД$(E, \varphi(N)) = 1$
4. Секретный ключ $D < N$; $E \cdot D = 1 \pmod{\varphi(N)}$

<u>Постановка подписи</u>

5. Вычисление хэш-функции $H = h(M)$, M - сообщение
6. Подпись $(M,S) \rightarrow S = H^{D} \pmod{N}$

<u>Проверка подписи</u>

7. Вычисление хэш-функции $H' = h(M)$
8. Вычисление $H'' = S^{E} \pmod{N}$
9. $H' = H''$?

Пример

<u>Генерация ключей</u>

1. $P = 3$, $Q = 11$
2. $N = 33$; $\varphi(N) = 20$
3. $E = 7$, НОД$(7, 20) = 1$
4. $D = 3$, $7 \cdot 3 = 1 \pmod{20}$

<u>Постановка подписи</u>

5. $H = 4$
6. $S = 4^{3} \pmod{33} = 31$

<u>Проверка подписи</u>

7. $H' = 4$
8. $H'' = 31^{7} \pmod{33} = 27512614111 \pmod{33} = 4$
9. $H' = H'' = 4$ – подпись верна

Схема шифрования ElGamal.

Пусть p – большое простое число, g – примитивный элемент мультипликативной группы GF(p), x случайное число, $x < p$-1.

$y = g^x \pmod p$ -открытый ключ,

x –секретный ключ.

Пусть надо зашифровать сообщение $M<p$:

1. Выбирается случайное число k, взаимно-простое с p - 1.
2. Затем вычисляется

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

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

Шифртекстом является пара (a, b).

При расшифровании вычисляется a^x и $b/a^x \pmod p$,

$$b/a^x \equiv y^k \cdot M/a^x \equiv g^{k\cdot x}\ M/g^{k\cdot x} \equiv M \pmod p$$

Подпись ElGamal.

Для генерации ключевой пары выбираются большое простое число p и примитивный элемент g мультипликативной группы GF(p). Выбирается случайное число x такое, что $x < p$-1.

Открытым ключом является $y = g^x \pmod p$; секретным ключом является x.

Схема ElGamal может быть использована для подписи в электронных деньгах и для зашифрования. Стойкость основана на сложности дискретного логарифмирования.

Пусть A должен подписать сообщение M. Выбирается случайное число k, взаимно-простое с p-1: НОД(k; p-1) = 1. Затем вычисляется $a = g^k \pmod p$.

Рассмотрим уравнение

$$M = (x \cdot a + k \cdot b) \pmod{(p-1)}.$$

По теореме о вычетах $\exists\, k^{-1}$: $(M\text{-}xa)\, k^{-1} \equiv b(\mathrm{mod}(p\text{-}1))$. Подписью под M является пара (a, b).

Проверка подписи:

Вычисляем $g^M\ (p)$ и $y^a \cdot a^b\ (p)$. Проверяем

$$y^a \cdot a^b \pmod p = g^{a\cdot x} \cdot g^{k\cdot b} \pmod p = g^{a\cdot x + k\cdot b} \pmod p =$$

$$= g^{ax+kk^{-1}(M-xa)+(p-1)nk} \pmod p = g^{M+(p-1)nk} \pmod p = g^M \pmod p.$$

ЭЦП ЭльГамаль. Пример

- [p,alpha,a,beta] = generateKeys
-
- message = 42
-
- [gamma,delta] = signature(message,alpha,p,a)
-
-
- signatureCheck(delta,gamma,beta,alpha,p,messag e)
-