

# Криптографические протоколы

## Лекция 7

### Протоколы распределения ключей (Часть 1)

Деркач Максим Юрьевич

November 26, 2019

1. ISO/IEC 11770-1:2010 – Information technology – Security techniques – Key management – Part 1: Framework
2. ISO/IEC 11770-2:2008 – Information technology – Security techniques – Key management – Part 2: Mechanisms using symmetric techniques
3. ISO/IEC 11770-3:2008 – Information technology – Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques
4. ISO/IEC 11770-4:2006 – Information technology – Security techniques – Key management – Part 4: Mechanisms based on weak secrets
5. СТБ 34.101.45-2013 "Информационные технологии и безопасность. Алгоритмы электронной цифровой подписи и транспорта ключа на основе эллиптических кривых".  
<http://apmi.bsu.by/assets/files/std/bign-spec19.pdf>
6. СТБ 34.101.60-2014 "Информационные технологии и безопасность. Алгоритмы разделения секрета".  
<http://apmi.bsu.by/assets/files/std/bols-spec12.pdf>

# Протоколы распределения ключей

## Определения и понятия

### Определение 1

Протокол распределения ключей (key establishment protocol)- это криптографический протокол, в процессе выполнения которого общий секрет доступен двум или более сторонам для последующего использования в криптографических целях.

Протоколы распределения ключей подразделяются на два класса:

- ▶ протоколы транспортировки ключей,
- ▶ протоколы обмена ключами.

### Определение 2

Протокол транспортировки ключей (key transport)- это протокол, распределения ключей, в котрых один участник создает или другим образом приобретает секрет и безопасным образом передает его другим участникам.

# Протоколы распределения ключей

## Определения и понятия

### Определение 3

Протокол обмена ключами (key exchange) - это протокол, распределения ключей, в котрых общий секрет вырабатывается двумя или более участниками как функция от информации.

### Классификация протоколов распределения ключей

► По типу выработки ключей:

1. обновление ключей (key update) - выработка совершенно нового ключа, не зависящего от ключей выработанных в прошлых сеансах выполнения ппротокола;
2. выработка производных ключей (key derivation) - вырабока нового ключа на основе уже существующих у участников криптосистемы.

# Протоколы распределения ключей

## Определения и понятия

### Классификация протоколов распределения ключей

#### ► По типу :

1. протоколы с предраспределенными ключами (key pre-distribution) - протоколы распределения, в которых результирующие ключи полностью определены априори начальным ключевым материалом (схемы разделения секрета);
2. протоколы динамического распределения ключей (dynamic key establishment) - протоколы распределения, в которых ключи, вырабатываемые участниками, различны в различных сеансах протокола.

#### ► По типу используемых криптосистем:

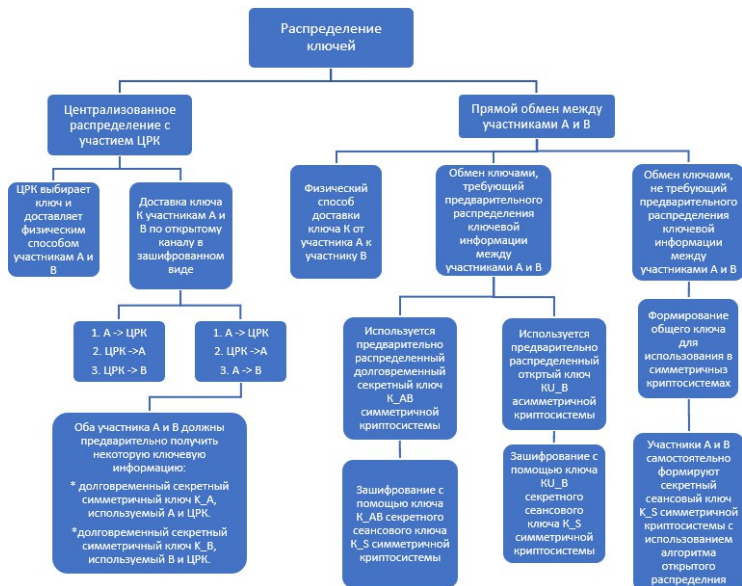
1. симметричные;
2. асимметричные.

#### ► По количеству сторон:

1. с участием "третьей стороны" (сервер аутентификации, центр распределения ключей, удостоверяющий центр и др.);
2. без участия "третьей стороны".

# Протоколы распределения ключей

## Классификация протоколов распределения ключей



# Протоколы распределения ключей

## Классификация протоколов распределения ключей

Классы протоколов	Протоколы распределения ключей			
	Транспортировка ключей	Обмен ключами		
Протоколы, основанные на симметричных криптосхемах	<i>Needham – Schroeder, Otway – Rees, Kerberos, Трехэтапный протокол Шамира</i>	<i>Шарады Меркле</i>	<i>Схема Блома</i>	<i>Схемы разделения секрета</i>
Протоколы, основанные на асимметричных криптосхемах	<i>Needham – Schroeder, X.509, Beller – Yacobi, SSL</i>	<i>Diffie – Hellman, ElGamal, MTI, STS, Gunther</i>	-	
	Динамическое распределение ключей		Протоколы с предраспределенными ключами	

## Мех. #2 (Однораундовый протокол)\*

1.  $A \rightarrow B : E_{K_{AB}}(KS)$

$A$  генерирует  $KS$ .

## Мех. #1 (Однораундовый протокол)\*

$TVP$  - переменная

1.  $A \rightarrow B : TVP$

$KS = f(K_{AB}, TVP)$ , где  $f$  - односторонняя функция.

## Мех. #3 (Однораундовый протокол)

1.  $A \rightarrow B : E_{K_{AB}}(KS || T_A/N_A || ID_B)$

$T_A/N_A$  - проверяет корректность момента времени или номера сессии.

$ID_B$  - против атаки отражения.



### Мех. #4 (Двухраундовый протокол)

1.  $B \rightarrow A : R_B$
2.  $A \rightarrow B : E_{K_{AB}}(KS || R_B || ID_B)$

### Мех. #4 (Модификация для двусторонней аутентификации)

1.  $B \rightarrow A : R_B$
2.  $A \rightarrow B : E_{K_{AB}}(KS || R_A || R_B || ID_B)$
3.  $B \rightarrow A : E_{KS}(R_A)$

### Мех. #6

$K_A$  - часть ключа  $KS$ , которая принадлежит  $A$ .

$K_B$  - часть ключа  $KS$ , которая принадлежит  $B$ .

$$KS = f(K_A, K_B)$$

1.  $B \rightarrow A : R_B$
2.  $A \rightarrow B : E_{K_{AB}}(K_A || R_A || R_B || ID_B)$
3.  $B \rightarrow A : E_{K_{AB}}(K_B || R_A || R_B)$

## Mech. #5

1.  $A \rightarrow B : E_{K_{AB}}(K_A || T_A / N_A || ID_B)$
2.  $B \rightarrow A : E_{K_{AB}}(K_B || T_B / N_B || ID_A)$

# Протоколы распределения ключей

## Бесключевой протокол Шамира (Трёхпроходный протокол Шамира)

### Коммутирующее шифрующее преобразование

$$\forall M, K_1, K_2 : E_{K_1}(E_{K_2}(M)) = E_{K_2}(E_{K_1}(M))$$

$E_K(M) = M \oplus K$  - слабое преобразование.

$E_{K_A}(M) = M^a \bmod p$ , где  $a$  - зависит от  $K_A$ ,  $p$  - простое.

1.  $A \rightarrow B : E_{K_A}(KS)$
2.  $B \rightarrow A : E_{K_B}(E_{K_A}(KS))$
3.  $A \rightarrow B : D_{K_A}(E_{K_B}(E_{K_A}(KS))) = E_{K_B}(KS)$

Отсутствует аутентификация, вместо  $B$  злоумышленник может вступить в протокол со своим ключом.

### Атака повторением (Replay Attack)

1.  $A \rightarrow B : E_{K_A}(KS)$
2.  $I(B) \rightarrow A : E_{K_A}(KS)$
3.  $A \rightarrow B : D_{K_A}(E_{K_A}(KS)) = KS$

Можно защитить протокол от этой атаки, осуществляя проверку на втором шаге с целью отбраковки повторно переданных сообщений.

Но, как заметил Карлсен (Carlsen), все равно можно осуществить атаку параллельного сеанса.

# Протоколы распределения ключей

## Трёхсторонние протоколы

### Wide-Mouth-Frog

1.  $A \rightarrow S : ID_A || E_{K_{AS}}(T_A || ID_B || KS)$
2.  $S \rightarrow B : E_{K_{BS}}(T_S || ID_A || KS)$

### Атака подмены типа

1.  $A \rightarrow S : ID_A || E_{K_{AS}}(T_A || ID_B || KS)$
2.  $S \rightarrow B : E_{K_{BS}}(T_S || ID_A || KS)$
3.  $I(B) \rightarrow S : ID_B || E_{K_{BS}}(T_S || ID_A || KS)$
4.  $S \rightarrow A : E_{K_{AS}}(T'_S || ID_B || KS)$
5.  $I(A) \rightarrow S : ID_A || E_{K_{AS}}(T'_S || ID_B || KS)$
6.  $S \rightarrow B : E_{K_{BS}}(T''_S || ID_A || KS)$

Цель атаки - злоумышленник может поддерживать ключи рабочими, в случае их компрометации.

# Протоколы распределения ключей

## Трёхсторонние протоколы

### Yahalom

1.  $A \rightarrow B : ID_A || R_A$
2.  $B \rightarrow S : ID_B || E_{K_{BS}}(ID_A || R_A || R_B)$
3.  $S \rightarrow A :$   
$$m_a = E_{K_{AS}}(ID_B || KS || R_A || R_B) ||$$
$$m_b = E_{K_{BS}}(ID_A || KS)$$
4.  $A \rightarrow B : m_b || E_{KS}(R_B)$

# Протоколы распределения ключей

## Трёхсторонние протоколы

### BAN-Yahalom

1.  $A \rightarrow B : ID_A || R_A$
2.  $B \rightarrow S : ID_B || R_B || E_{K_{BS}}(ID_A || R_A)$
3.  $S \rightarrow A : R_B ||$   
 $m_a = E_{K_{AS}}(ID_B || KS || R_A) ||$   
 $m_b = E_{K_{BS}}(ID_A || KS || R_B)$
4.  $A \rightarrow B : m_b || E_{KS}(R_B)$

### Атака чередования сеансов и подмены типов

1.  $I(A) \rightarrow B : ID_A || R_A$
2.  $B \rightarrow I(S) : ID_B || R_B || E_{K_{BS}}(ID_A || R_A)$
- 1'  $I(A) \rightarrow B : ID_A || (R_A || R_B)$
- 2'  $B \rightarrow I(S) : ID_B || R'_B || E_{K_{BS}}(ID_A || (R_A || R_B))$
3. — — — — —
4.  $I(A) \rightarrow B : E_{K_{BS}}(ID_A || R_A || R_B) || E_{R_A}(R_B)$

## Needham-Schroeder (NSSK)

1.  $A \rightarrow S : ID_A || ID_B || R_A$
2.  $S \rightarrow A : E_{K_{AS}}(R_A || ID_B || KS || E_{K_{BS}}(KS || ID_A))$
3.  $A \rightarrow B : E_{K_{BS}}(KS || ID_A)$
4.  $B \rightarrow A : E_{KS}(R_B)$
5.  $A \rightarrow B : E_{KS}(R_B - 1)$



### Атака повторением (Replay Attack)

Если ключ  $KS$  скомпрометирован, возможна атака на протокол методом повтора сеанса: берутся сообщения из прошлого сеанса с ключом  $KS^*$ :

1.  $A \rightarrow S : ID_A || ID_B || R_A$
2.  $S \rightarrow A : E_{K_{AS}}(R_A || ID_B || KS || E_{K_{BS}}(KS || ID_A))$
3.  $I(A) \rightarrow B : E_{K_{BS}}(KS^* || ID_A)$
4.  $B \rightarrow I(A) : E_{KS^*}(R_B)$
5.  $I(A) \rightarrow B : E_{KS^*}(R_B - 1)$

## Протокол Деннинг - Сакко\*

1.  $A \rightarrow S : ID_A || ID_B$
2.  $S \rightarrow A : E_{K_{AS}}(ID_B || KS || T_S || E_{K_{BS}}(ID_A || KS || T_S))$
3.  $A \rightarrow B : E_{K_{BS}}(ID_A || KS || T_S)$
4.  $B \rightarrow A : E_{KS}(R_B)$
5.  $A \rightarrow B : E_{KS}(R_B - 1)$

1.  $A \rightarrow B : ID_A$
2.  $B \rightarrow A : E_{K_{BS}}(ID_A || R_B)$
3.  $A \rightarrow S : ID_A || ID_B || R_A || E_{K_{BS}}(ID_A || R_B)$
4.  $S \rightarrow A : E_{K_{AS}}(R_A || ID_B || KS || E_{K_{BS}}(KS || R_B || ID_A))$
5.  $A \rightarrow B : E_{K_{BS}}(KS || R_B || ID_A)$
6.  $B \rightarrow A : E_{KS}(R'_B)$
7.  $A \rightarrow B : E_{KS}(R'_B - 1)$

## Протокол Отвея - Рисса

$M$  - ID сеанса.

1.  $A \rightarrow B : M || ID_A || ID_B || E_{K_{AS}}(R_A || M || ID_A || ID_B)$
2.  $B \rightarrow S :$   
 $M || ID_A || ID_B || E_{K_{AS}}(R_A || M || ID_A || ID_B) || E_{K_{BS}}(R_B || M || ID_A || ID_B)$
3.  $S \rightarrow B : M || E_{K_{AS}}(R_A || KS) || E_{K_{BS}}(R_B || KS)$
4.  $B \rightarrow A : M || E_{K_{AS}}(R_A || KS)$

# Протоколы распределения ключей

## Атака 1

$KS$  - 64 бита,  $M$  - 32 бита,  $ID_A, ID_B$  - 16 бит.

$$\text{len}(KS) = \text{len}(M + ID_A + ID_A)$$

$$1' \quad A \rightarrow I(B) : M || ID_A || ID_B || E_{K_{AS}}(R_A || M || ID_A || ID_B)$$

$$4' \quad I(B) \rightarrow A : M || E_{K_{AS}}(R_A || M || ID_A || ID_B)$$

## Атака 2

$$1. \quad A \rightarrow B : M || ID_A || ID_B || E_{K_{AS}}(R_A || M || ID_A || ID_B)$$

$$2. \quad B \rightarrow I(S) : \\ M || ID_A || ID_B || E_{K_{AS}}(R_A || M || ID_A || ID_B) || E_{K_{BS}}(R_B || M || ID_A || ID_B)$$

$$3. \quad I(S) \rightarrow B : \\ M || E_{K_{AS}}(R_A || M || ID_A || ID_B) || E_{K_{BS}}(R_B || M || ID_A || ID_B)$$

$$4. \quad B \rightarrow A : M || E_{K_{AS}}(R_A || M || ID_A || ID_B)$$

## Mech. #10\*

1.  $A \rightarrow S : TVP_A || ID_B$
2.  $S \rightarrow A :$   
 $E_{K_{AS}}(TVP_A || KS || ID_B || text_1) || E_{K_{BS}}(T_S / N_S || KS || ID_A || text_2) ||$
3.  $A \rightarrow B :$   
 $E_{K_{BS}}(T_S / N_S || KS || ID_A || text_2) || E_{KS}(T_A / N_A || ID_B || text_3)$
4.  $B \rightarrow A : E_{KS}(T_B / N_B || ID_A || text_4)$

# Протоколы распределения ключей

## Протоколы основанные на асимметричных криптосистемах

### Needham-Schroeder Public Key (NSPK)

1.  $A \rightarrow S : ID_A || ID_B$
2.  $S \rightarrow A : E_{K_S^{sec}}(K_B^{pub} || ID_B)$
3.  $A \rightarrow B : E_{K_B^{pub}}(K_A || ID_A)$
4.  $B \rightarrow S : ID_B || ID_A$
5.  $S \rightarrow B : E_{K_S^{sec}}(K_A^{pub} || ID_A)$
6.  $B \rightarrow A : E_{K_A^{pub}}(K_B || K_A)$
7.  $A \rightarrow B : E_{K_B^{pub}}(K_B)$
8.  $A, B : KS = f(K_A, K_B)$

$E_{K_S^{sec}}()$  - подпись на секретном ключе.

$E_{K_B^{pub}}()$  - шифрование на открытом ключе.

$f()$  - общеизвестная однонаправленная функция.

# Протоколы распределения ключей

## Протоколы основанные на асимметричных криптосистемах

### NSPK без 3-ей стороны

1.  $A \rightarrow B : E_{K_B^{pub}}(K_A || ID_A)$
2.  $B \rightarrow A : E_{K_A^{pub}}(K_A || K_B)$
3.  $A \rightarrow B : E_{K_B^{pub}}(K_B)$
4.  $A, B : KS = f(K_A, K_B)$

# Протоколы распределения ключей

## Смешанные протоколы

### EKE(Encrypted Key Exchange)

$K_{AB} = P$  - пароль

1.  $A \rightarrow B : ID_A || E_P(K_A^{pub})$
2.  $B \rightarrow A : E_P(E_{K_A^{pub}}(KS))$
3.  $A \rightarrow B : E_{KS}(R_A)$
4.  $B \rightarrow A : E_{KS}(R_A || R_B)$
5.  $A \rightarrow B : E_{KS}(R_B)$

### Bilateral Key Exchange with Public Key\*

1.  $B \rightarrow A : ID_B || E_{K_A^{pub}}(R_B || ID_B)$
2.  $A \rightarrow B : E_{K_B^{pub}}(h(R_B) || R_A || ID_A || KS)$
3.  $B \rightarrow A : E_{KS}(h(R_A))$



# Протоколы распределения ключей

## Протоколы с использованием ЭЦП

### Сертификаты открытых ключей

$$cert_A = (ID_A || K_A^{pub} || t || sign_T(ID_A || K_A^{pub} || t))$$

### X.509

$$d_A = (T_A || R_A || ID_B || text_1 || E_{K_B^{pub}}(K_A))$$

$$d_B = (T_B || R_B || ID_A || text_2 || E_{K_A^{pub}}(K_B))$$

1.  $A \rightarrow B : cert_A || d_A || sign_A(d_A)$
2.  $B \rightarrow A : cert_B || d_B || sign_B(d_B)$
3.  $A \rightarrow B : R_B || ID_B || sign_A(R_B || ID_B)$
4.  $A, B : KS = f(K_A, K_B)$

Шаг (3) необязателен, выполняется только если нужно подтверждение.

# Протоколы распределения ключей

## Протоколы с использованием ЭЦП

### Денниг -Сакко\*

1.  $A \rightarrow S : ID_A || ID_B$
2.  $S \rightarrow A : cert_A || cert_B$
3.  $A \rightarrow B : cert_A || cert_B || E_{K_B^{pub}}(KS || t_A || sign_A(kS || T_A))$
4.  $A, B : KS = f(K_A, K_B)$

# Протоколы распределения ключей

## Протокол МТІ

### 1. Предварительный этап:

Выбираются следующие параметры:  $p, \alpha$ , где  $p$  - простое число,  $a \in Z_p^*$

$A$  выбирает  $a$ ,  $1 \leq a \leq p-2$ ,  $z_A = \alpha^a \pmod{p}$ .

$B$  выбирает  $b$ ,  $1 \leq b \leq p-2$ ,  $z_B = \alpha^b \pmod{p}$ .

### 2. $A \rightarrow B : m_{AB} = \alpha^x \pmod{p}$ , $1 \leq x \leq p-2$ , $x$ - случайное

### 3. $B \rightarrow A : m_{BA} = \alpha^y \pmod{p}$ , $1 \leq y \leq p-2$ , $y$ - случайное

Варианты построения ключа:

№	$m_{AB}$	$m_{BA}$	$K_A$	$K_B$	$K$
1	$\alpha^x$	$\alpha^y$	$m_{BA}^a z_B^x$	$m_{AB}^b z_A^y$	$\alpha^{bx+ay}$
2	$z_B^x$	$z_A^y$	$m_{BA}^{a^{-1}} \alpha^x$	$m_{AB}^{b^{-1}} \alpha^y$	$\alpha^{x+y}$
3	$z_B^x$	$z_A^y$	$m_{BA}^{a^{-1}x}$	$m_{AB}^{b^{-1}y}$	$\alpha^{xy}$
4	$z_B^x$	$z_A^y$	$m_{BA}^x$	$m_{AB}^y$	$\alpha^{bxay}$

