

# Криптографические протоколы

## Лекция 5

### Протоколы "сильной" аутентификации

Деркач Максим Юрьевич

September 27, 2018

# Ссылки

# Классификация протоколов "сильной" аутентификации

- \* на основе симметричных алгоритмов шифрования;
- \* на основе асимметричных алгоритмов шифрования;
- \* на основе ЭЦП.

# Протоколы "сильной" аутентификации

На основе симметричных алгоритмов шифрования

## ISO/ IEC 9798 - 2

1.  $A \rightarrow B : text_2 || E_{K_{AB}}(T_A/N_A || ID_B || text_1)$

2.  $B \rightarrow A : text_4 || E_{K_{AB}}(T_B/N_B || ID_A || text_3)$

1.  $B \rightarrow A : R_B || text_1$

2.  $A \rightarrow B : text_3 || E_{K_{AB}}(R_B || ID_B || text_2)$

1.  $B \rightarrow A : R_B || text_1$

2.  $A \rightarrow B : text_3 || E_{K_{AB}}(R_A || R_B || ID_B || text_2)$

3.  $B \rightarrow A : text_5 || E_{K_{AB}}(R_B || R_A || text_4)$

**Замечание** Длина  $ID_B || text_2$  не должна равняться длине  $text_4$

# Протоколы "сильной" аутентификации

На основе симметричных алгоритмов шифрования

## Протокол Ву-Лама (Woo-Lam)

1.  $A \rightarrow B : ID_A$
2.  $B \rightarrow A : R_B$
3.  $A \rightarrow B : E_{K_{AT}}(R_B)$
4.  $B \rightarrow T : E_{K_{BT}}(ID_A || E_{K_{AT}}(R_B))$
5.  $T \rightarrow B : E_{K_{BT}}(R_B)$

# Протоколы "сильной" аутентификации

На основе симметричных алгоритмов шифрования

## Атака параллельного сеанса

- 1  $I(A) \rightarrow B : ID_A$
- 1'  $I \rightarrow B : ID_I$
- 2  $B \rightarrow I(A) : R_B$
- 2'  $B \rightarrow I : R_B^*$
- 3  $I(A) \rightarrow B : E_{K_{IT}}(R_B)$
- 3'  $I \rightarrow B : E_{K_{IT}}(R_B)$
- 4  $B \rightarrow T : E_{K_{BT}}(ID_A || E_{K_{IT}}(R_B))$
- 4'  $B \rightarrow T : E_{K_{BT}}(ID_I || E_{K_{IT}}(R_B))$
- 5  $T \rightarrow B : E_{K_{BT}}("MYCOP")$
- 5'  $T \rightarrow B : E_{K_{BT}}(R_B)$

# Протоколы "сильной" аутентификации

На основе симметричных алгоритмов шифрования

## Протокол Отвея-Риса

1.  $A \rightarrow B : ID_A || ID_B || K_{AT}(ID_A || ID_B || N_A || R_A) || N_A$
2.  $B \rightarrow T : ID_A || ID_B || K_{AT}(ID_A || ID_B || N_A || R_A) ||$   
 $K_{BT}(ID_A || ID_B || N_A || R_B) || N_A$
3.  $T \rightarrow B : E_{K_{AT}}(K || R_A) || E_{K_{BT}}(K || R_B) || N_A$
4.  $B \rightarrow A : E_{K_{AT}}(K || R_A) || E_K(R_A || R_B) || N_A$
5.  $A \rightarrow B : E_K(R_B)$

## Протокол с использованием хэш-функции

1.  $B \rightarrow A : R_B || text_1$
2.  $A \rightarrow B : text_3 || H_{K_{AB}}(R_A || R_B || ID_B || text_2)$
3.  $B \rightarrow A : text_5 || H_{K_{AB}}(R_B || R_A || ID_A || text_4)$

# Протоколы "сильной" аутентификации

На основе асимметричных алгоритмов шифрования

## С использованием хэш-функции

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

## NSPK

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



# Протоколы "сильной" аутентификации

На основе асимметричных алгоритмов шифрования

## Атака параллельного сеанса NSPK

$$1 \quad A \rightarrow I : E_{K_I^{pub}}(R_A || ID_A)$$

$$1' \quad I(A) \rightarrow B : E_{K_B^{pub}}(R_A || ID_A)$$

$$2 \quad B \rightarrow I(A) : E_{K_A^{pub}}(R_A || R_B)$$

$$2' \quad I \rightarrow A : E_{K_A^{pub}}(R_A || R_B)$$

$$3 \quad A \rightarrow I : E_{K_I^{pub}}(R_B)$$

$$3' \quad I(A) \rightarrow B : E_{K_B^{pub}}(R_B)$$

## Защита

$$\blacktriangleright \quad 2 \quad B \rightarrow A : E_{K_A^{pub}}(R_A || R_B || ID_B)$$

$$\blacktriangleright \quad 3 \quad A \rightarrow B : E_{K_{h(R_B)}}(ID_B)$$

# Протоколы "сильной" аутентификации

С использованием ЭЦП

1.  $A \rightarrow B :$

$cert_A || T_A / N_A || ID_B || text_2 || sign_A(T_A / N_A || ID_B || text_1)$

2.  $B \rightarrow A :$

$cert_B || T_B / N_B || ID_A || text_4 || sign_B(T_B / N_B || ID_A || text_3)$

1.  $B \rightarrow A : R_B || text_1$

2.  $A \rightarrow B :$

$cert_A || R_A || R_B || ID_B || text_3 || sign_A(R_A || R_B || ID_B || text_2)$

3.  $B \rightarrow A :$

$cert_B || R_B || R_A || ID_A || text_5 || sign_B(R_B || R_A || ID_A || text_4)$

# Протоколы "сильной" аутентификации

С использованием ЭЦП

## Атака

1.  $I(B) \rightarrow A : R_B$
2.  $A \rightarrow I(B) : cert_A || R_A || R_B || ID_B || sign_A(R_A || R_B || ID_B)$
- 1'  $I(A) \rightarrow B : R_A$
- 2'  $B \rightarrow I(A) : cert_B || R'_B || R_A || ID_A || sign_B(R'_B || R_A || ID_A)$
3.  $I(B) \rightarrow A : cert_B || R'_B || R_A || ID_A || sign_B(R'_B || R_A || ID_A)$



