

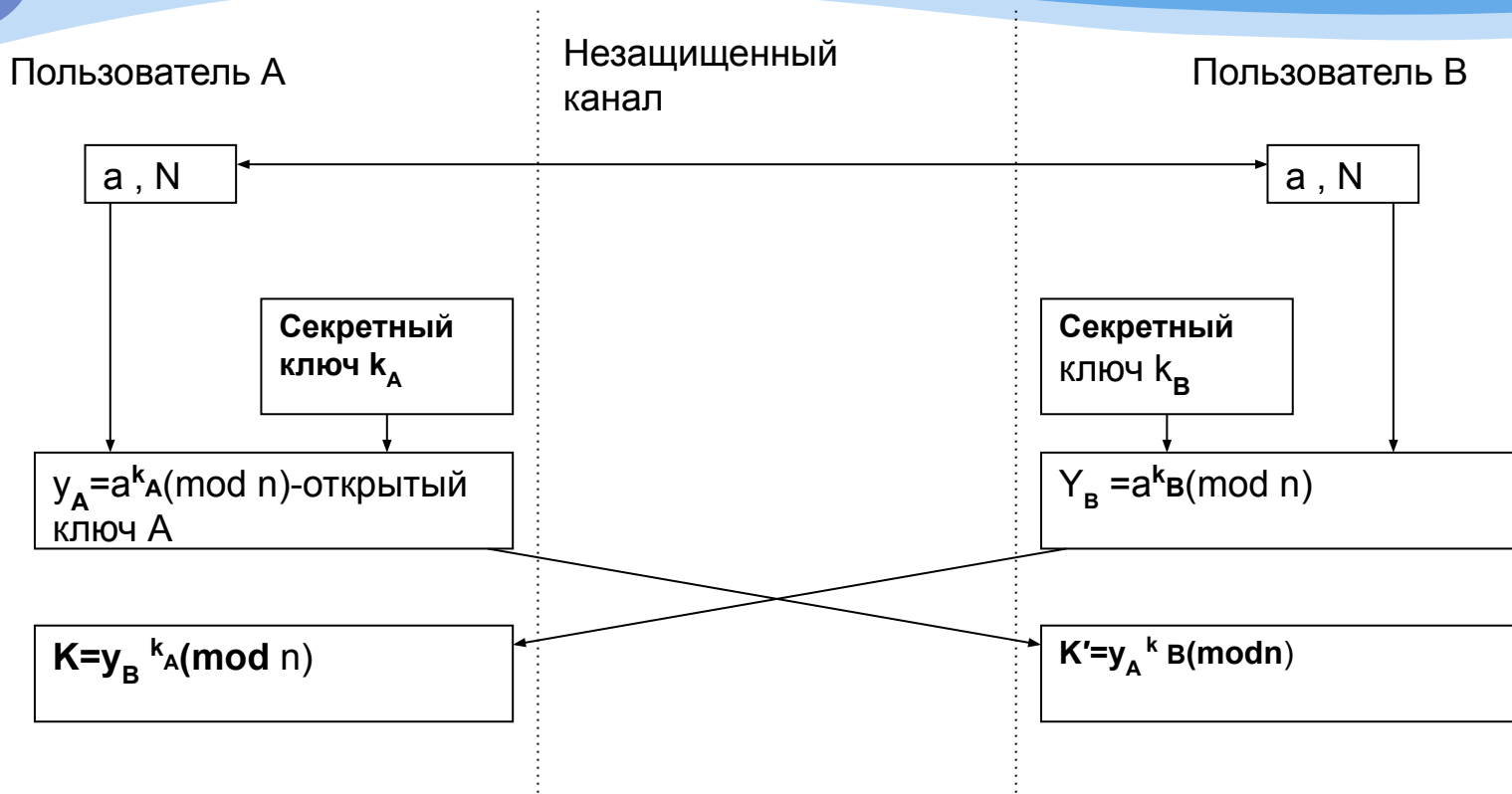
# СИСТЕМЫ УПРАВЛЕНИЯ КРИПТОГРАФИЧЕСКИМИ КЛЮЧАМИ

Лекция 12

# Прямой обмен ключами между пользователями

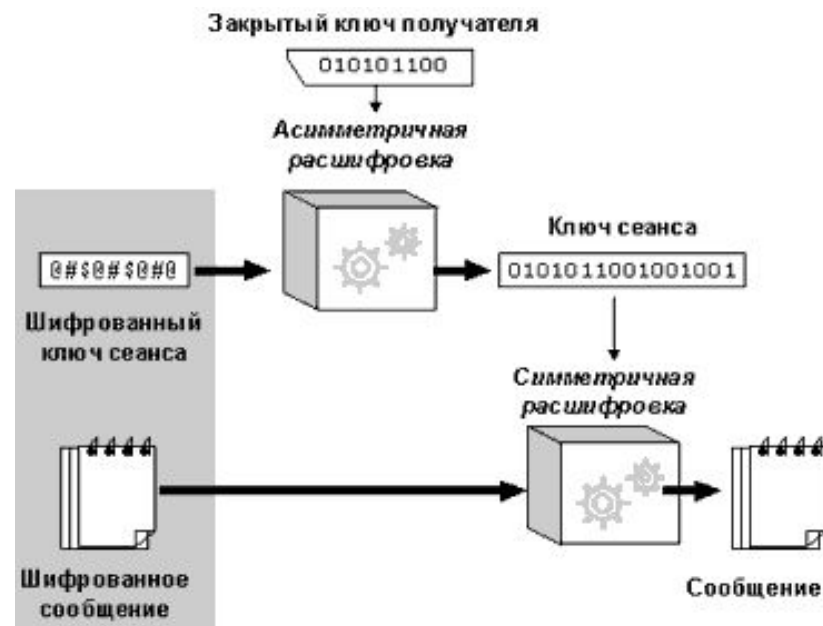
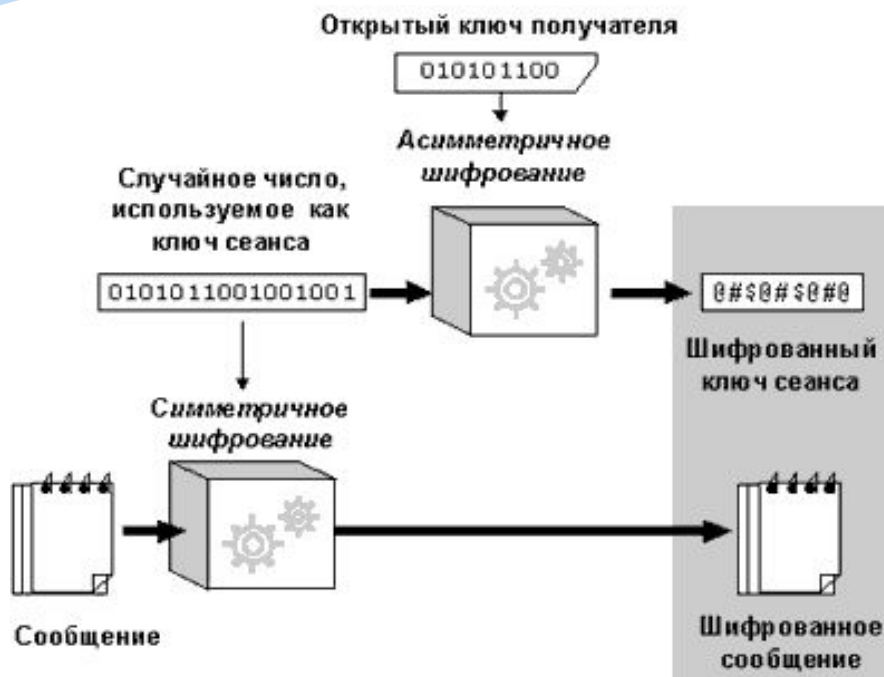


# Схема реализации алгоритма Диффи-Хеллмана



$N$  – простое,  $a \in \mathbb{Z}_N, (1 \leq a \leq N-1)$ ;  
 $K = K' = a^{k_A k_B} \pmod n$

# Электронный цифровой конверт



# Электронный цифровой конверт

■ А ЭЦК  $\longrightarrow$  В

❖ М – сообщение  $K^c = D_{K_B^c}(C_K)$

❖  $C_m(M) = E_K^c(M)$   $M = D_K^c(C_m)$

❖  $C_K(K^c) = E_{K_B^0}(K^c)$

❖ Е-шифрование, D-расшифрование,

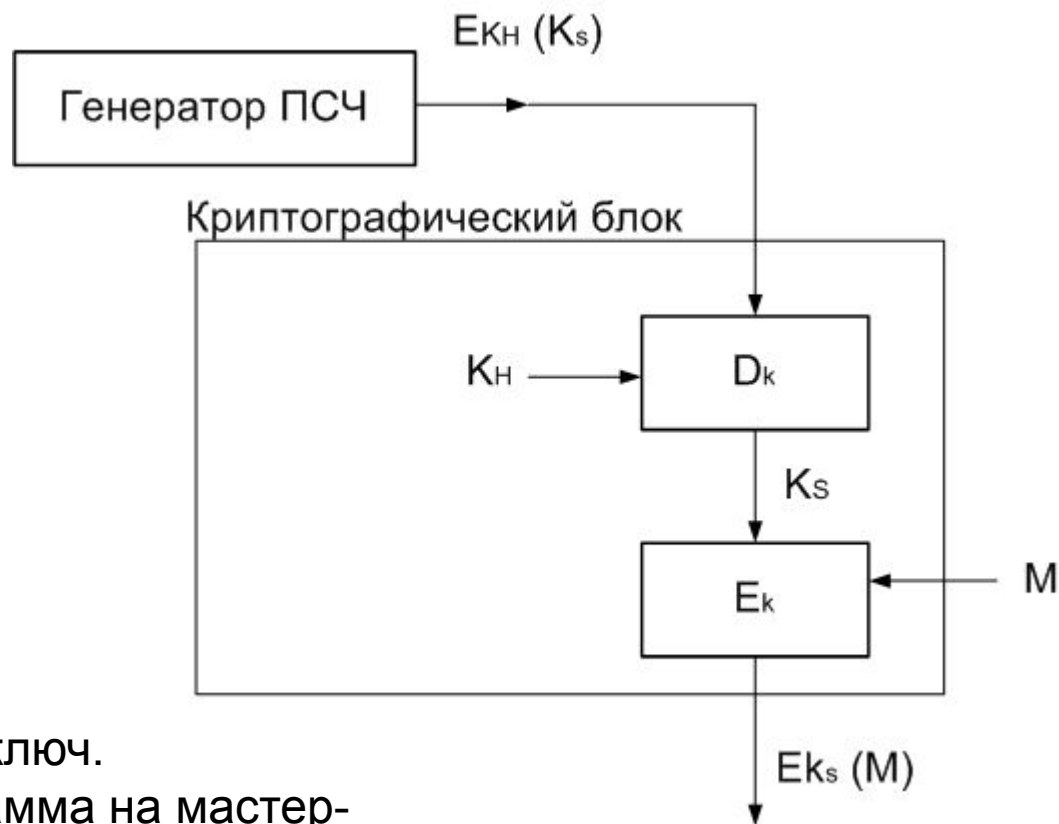
❖  $K^c$ -симметричный секретный ключ,  $K_B^0$  – открытый ключ В,  $K_B^c$  – секретный ключ В.

# Хранение ключей

- ❖ Ключи хранят в зашифрованном виде на диске, Touch Memory и в пластиковых картах.
- ❖ **Стандарт ISO 8532** – устанавливает иерархию ключей, она может быть двух- и трехуровневой.
- ❖ **Двухуровневая:**
  - ❖ Ключи для шифрования ключей (КК)
  - ❖ Ключи данных (ключи сеансовые, ключи рабочие) (КД)
- ❖ **Трехуровневая:**
  - ❖ Главные, мастер - ключи (ГК)
  - ❖ КК
  - ❖ КД
- ❖ Кроме иерархии, стандартом устанавливаются и сроки хранения.
- ❖ ГК - доставляется при личном контакте, хранится от нескольких недель до месяцев в защищенной от сбоев и прочной криптосистеме.
- ❖ КД – в идеале должен меняться после каждого сеанса связи. Если ключи рабочие применяются для шифрования файлов, то срок действия может составлять несколько часов.



# Хранение ключей



$K_H$  – новый мастер-ключ.

$E_{K_H}(K_S)$  – криптограмма на мастер-ключе. Расшифровывается перед использованием  $K_S$ .

$M$  – шифруемое сообщение