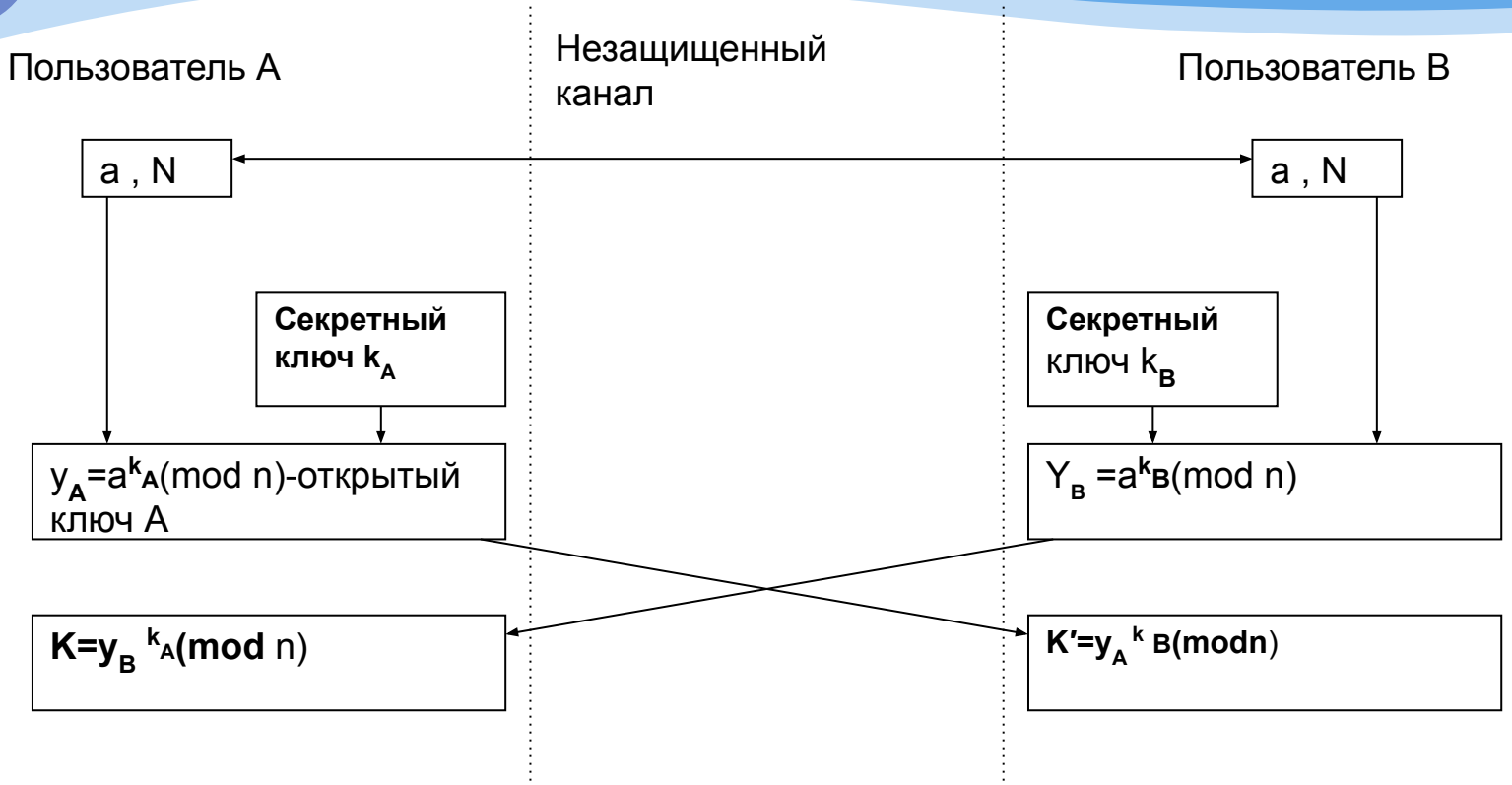
СИСТЕМЫ УПРАВЛЕНИЯ КРИПТОГРАФИЧЕСКИМИ КЛЮЧАМИ

Лекция 12

Прямой обмен ключами между пользователями

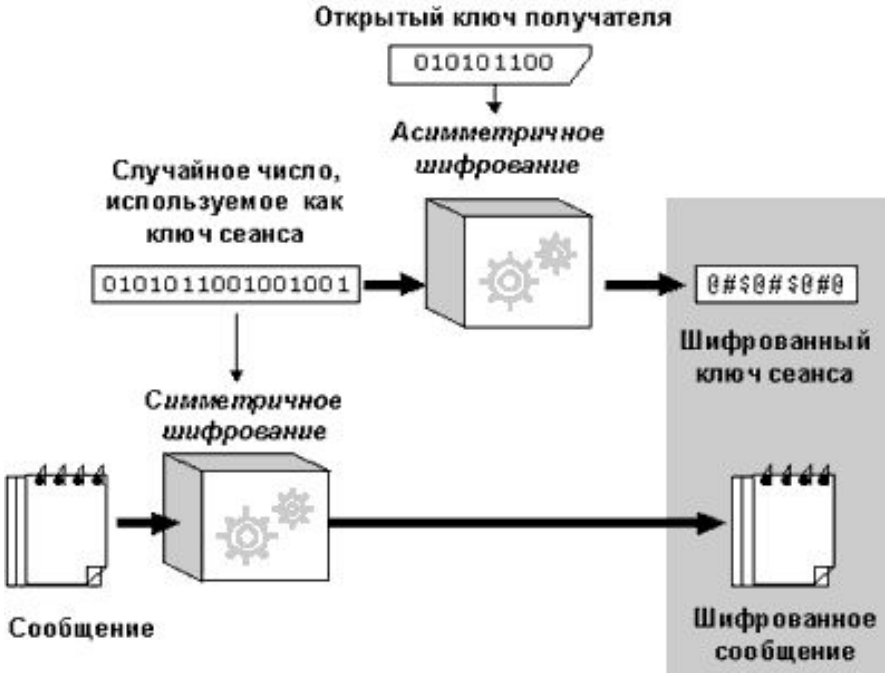
Схема реализации алгоритма Диффи-Хеллмана

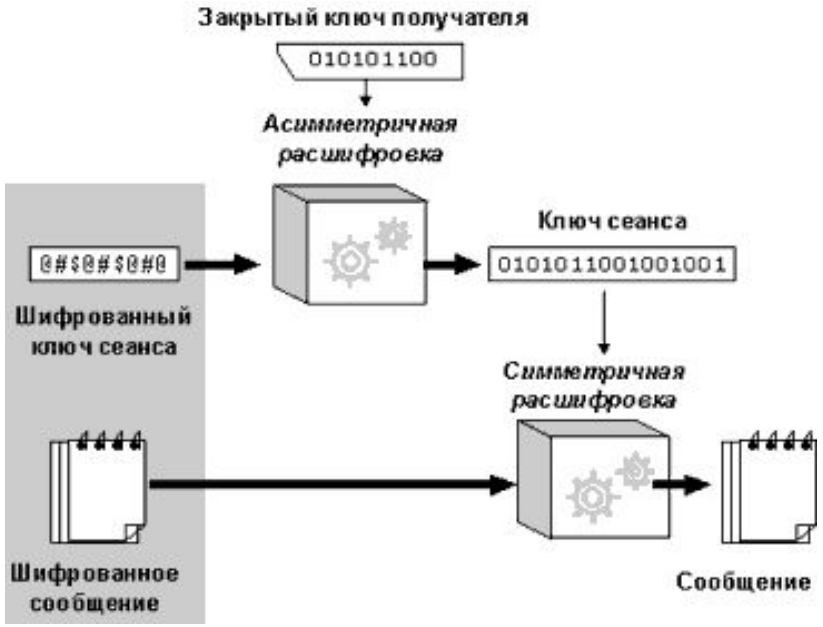


N – простое, $a \in Z_N$,$(1 \le a \le N-1)$;

$K=K'=a^{k_A k_B}(\mathbf{mod}\ n)$

Электронный цифровой конверт





Электронный цифровой конверт

- A ЭЦК ⟶ B

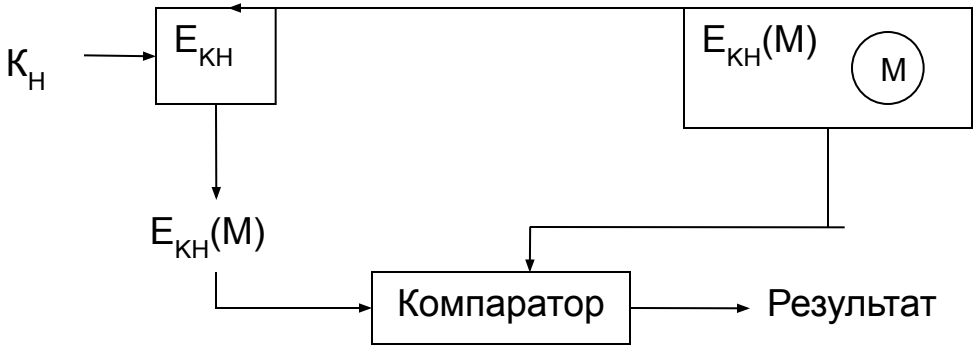
- M – сообщение $К^{с}=D_{Кв}{}^{с}(С_{к})$
- $С_{m}(M)=E_{к}{}^{с}(M)$ $M=D_{k}{}^{с}(С_{m})$
- $С_{k}(К^{с})=E_{Кв}{}^{о}(К^{с})$

- E-шифрование, D-расшифрование,
- $К^{с}$-симметричный секретный ключ, $К_{в}{}^{о}$ – открытый ключ B, $К_{в}{}^{с}$–секретный ключ B.

Хранение ключей

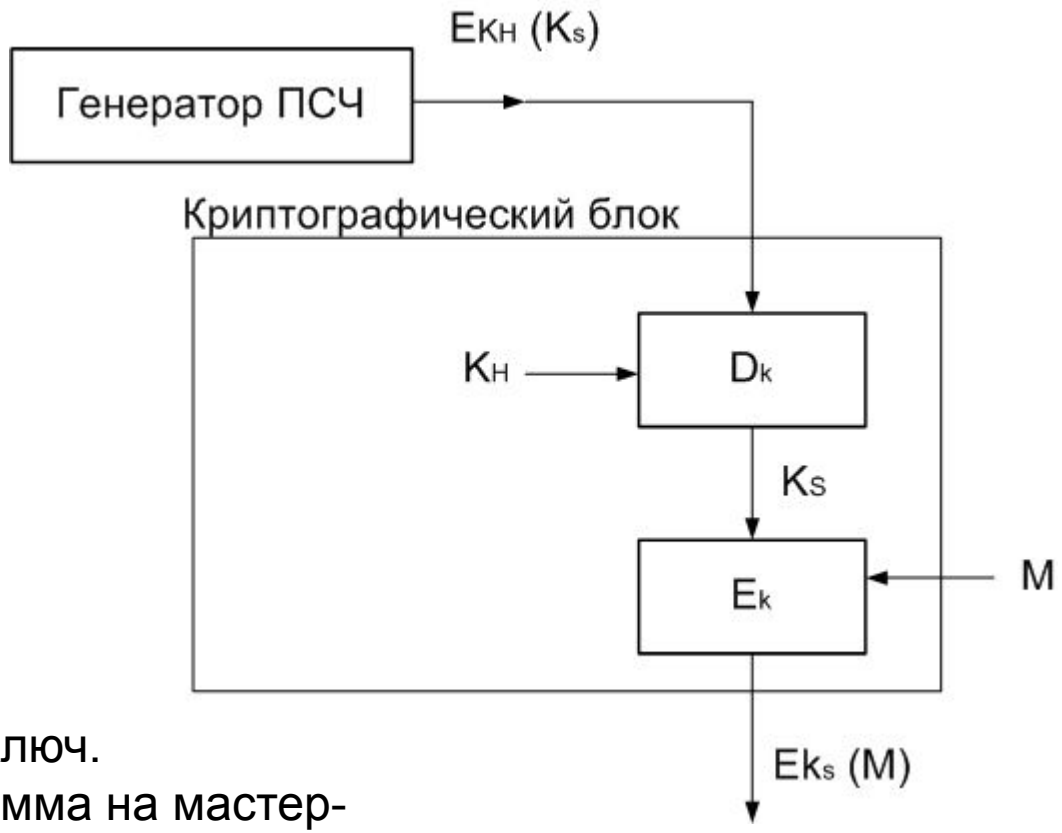
- Ключи хранят в зашифрованном виде на диске, Touch Memory и в пластиковых картах.
- **Стандарт ISO 8532** – устанавливает иерархию ключей, она может быть двух- и трехуровневой.
- **Двухуровневая:**
- Ключи для шифрования ключей (КК)
- Ключи данных (ключи сеансовые, ключи рабочие) (КД)
- **Трехуровневая:**
- 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.

Проверка ключей



Кн – новый ключ
M – некое хранящееся значение.
На Кн зашифровывается и хранится криптограмма.
Периодически она делается заново и сравнивается с хранящимся.
Количество ключей для связи с N пользователями должно быть равно N*(N-1) – общее количество для всех пользователей

Хранение ключей



Кн – новый мастер-ключ.
Ekн (Ks) – криптограмма на мастер-ключе. Расшифровывается перед использованием Ks.
M – шифруемое сообщение