Кафедра № 12 Компьютерные системы и технологии
НИЯУ МИФИ

Защита информации

Иванов М.А.

Лекция № 7.
Криптографические протоколы

Москва, 2025

КС&Т

Кафедра № 12 Компьютерные системы и технологии
НИЯУ МИФИ

Защита информации

Иванов М.А.

Лекция № 7.
Криптографические протоколы

Темы

- Примитивные и прикладные криптографические протоколы
- Протокол электронной подписи (ЭП)
- Протоколы аутентификации удаленных абонентов
- Протокол разделения секрета
- Протоколы доказательства с нулевым разглашением знаний
- Протокол подбрасывания монеты

Повторение

- Односторонняя функция
- Протокол выработки общего секретного ключа Диффи-Хеллмана
- Односторонняя функция с секретом
- Криптосистема с открытым ключом
- Криптосистема RSA
- Идея электронной подписи

Криптографические протоколы

Протоколы

- Прикладные
- Примитивные

Криптографические протоколы

Протоколы

- Прикладные
- Примитивные

Интерактивный протокол

- Распределенный алгоритм - описание характера и последовательности действий каждого из участников
- Спецификация форматов пересылаемых сообщений
- Спецификация синхронизации действий участников
- Описание действий при возникновении сбоев

Криптографические протоколы

Интерактивная система доказательств (P, V, S)
Interactive Proof System

- Полнота – если утверждение *S* действительно истинно, то доказывающий P сможет убедить проверяющего V признать это
- Корректность – если *S* ложно, то доказывающий не сможет убедить проверяющего в обратном

P может быть противником

Криптографические протоколы

Интерактивная система доказательств (*P*, *V*, *S*)
Interactive Proof System

- Полнота – если утверждение *S* действительно истинно, то доказывающий *P* сможет убедить проверяющего *V* признать это
- Корректность – если *S* ложно, то доказывающий не сможет убедить проверяющего в обратном

P может быть противником

Доказательство с нулевым разглашением знаний (P, V, S)
Zero-Knowledge Proofs

- Полнота
- Корректность
- Нулевое разглашение – в результате работы протокола *V* не увеличит своих знаний об утверждении *S*

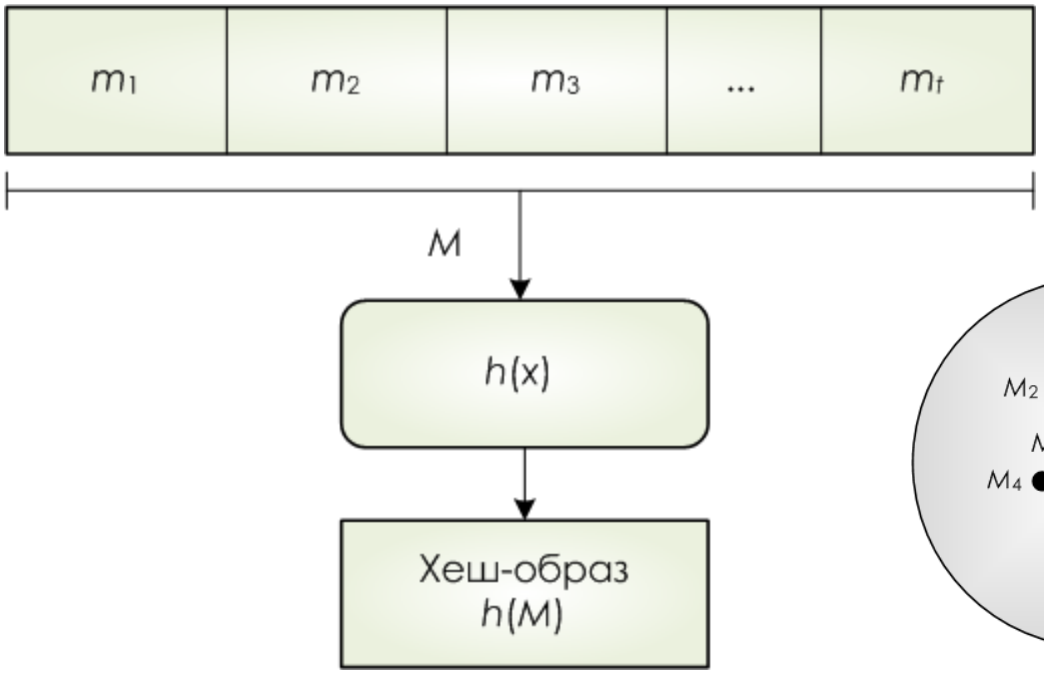
V может быть противником

Протокол электронной подписи

Схема ЭП

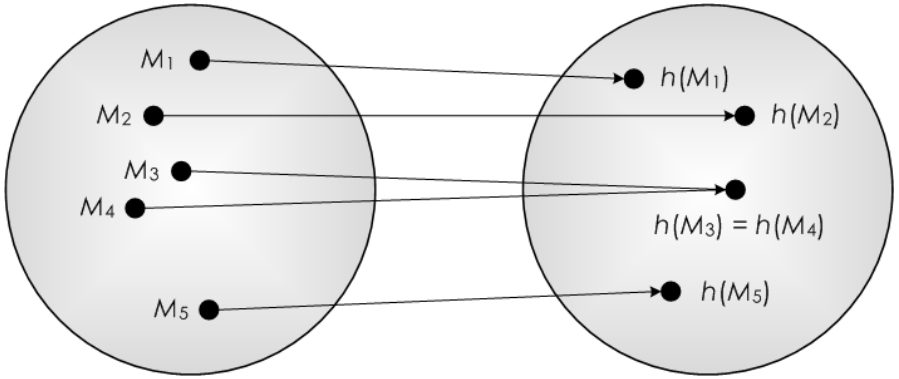
- Параметр безопасности
- Пространство исходных сообщений
- Максимальное число подписей (Signature Bound)
- Алгоритм G генерации ключей (SK, PK)
- Алгоритм S формирования подписи сообщения
- Алгоритм V проверки подписи

Хеш-функция: *a* - принцип действия; *b* - множества прообразов и хеш-образов



a

$|M| > |h(M)|$,
$|M| < |h(M)|$,
$|M| = |h(M)|$



b

Хеш-функция: требования

- При заданном значении M задача нахождения $h(M)$ должна быть вычислительно разрешима

Хеш-функция: требования

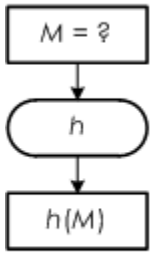
- При заданном значении M задача нахождения $h(M)$ должна быть вычислительно разрешима
- $h(M)$ должен зависеть от всех бит прообраза M и от их взаимного расположения

Хеш-функция: требования

- При заданном значении *M* задача нахождения *h*(*M*) должна быть вычислительно разрешима
- *h*(*M*) должен зависеть от всех бит прообраза *M* и от их взаимного расположения
- Результат действия ХФ должен быть непредсказуем

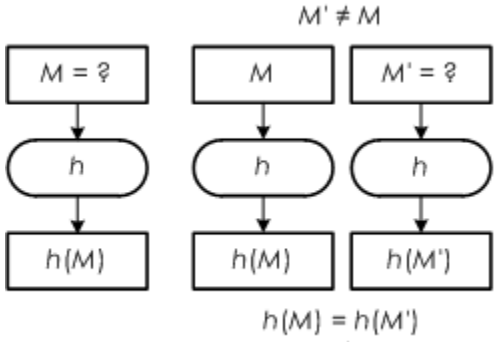
Хеш-функция: требования

- При заданном значении *M* задача нахождения *h*(*M*) должна быть вычислительно разрешима
- *h*(*M*) должен зависеть от всех бит прообраза *M* и от их взаимного расположения
- Результат действия ХФ должен быть непредсказуем
- При заданном значении *h*(*M*) задача нахождения *M* должна быть вычислительно неразрешимой (**pre-image resistance**)



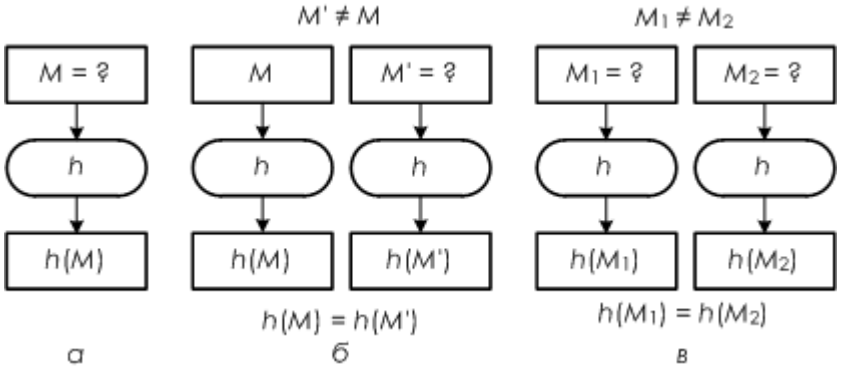
Хеш-функция: требования

- При заданном значении M задача нахождения $h(M)$ должна быть вычислительно разрешима
- $h(M)$ должен зависеть от всех бит прообраза M и от их взаимного расположения
- Результат действия ХФ должен быть непредсказуем
- При заданном значении $h(M)$ задача нахождения M должна быть вычислительно неразрешимой (**pre-image resistance**)
- При заданных значениях $h(M)$ и первого прообраза M задача нахождения второго прообраза $M' \neq M$, такого, что $h(M') = h(M)$, должна быть вычислительно неразрешимой (**second pre-image resistance**)



Хеш-функция: требования

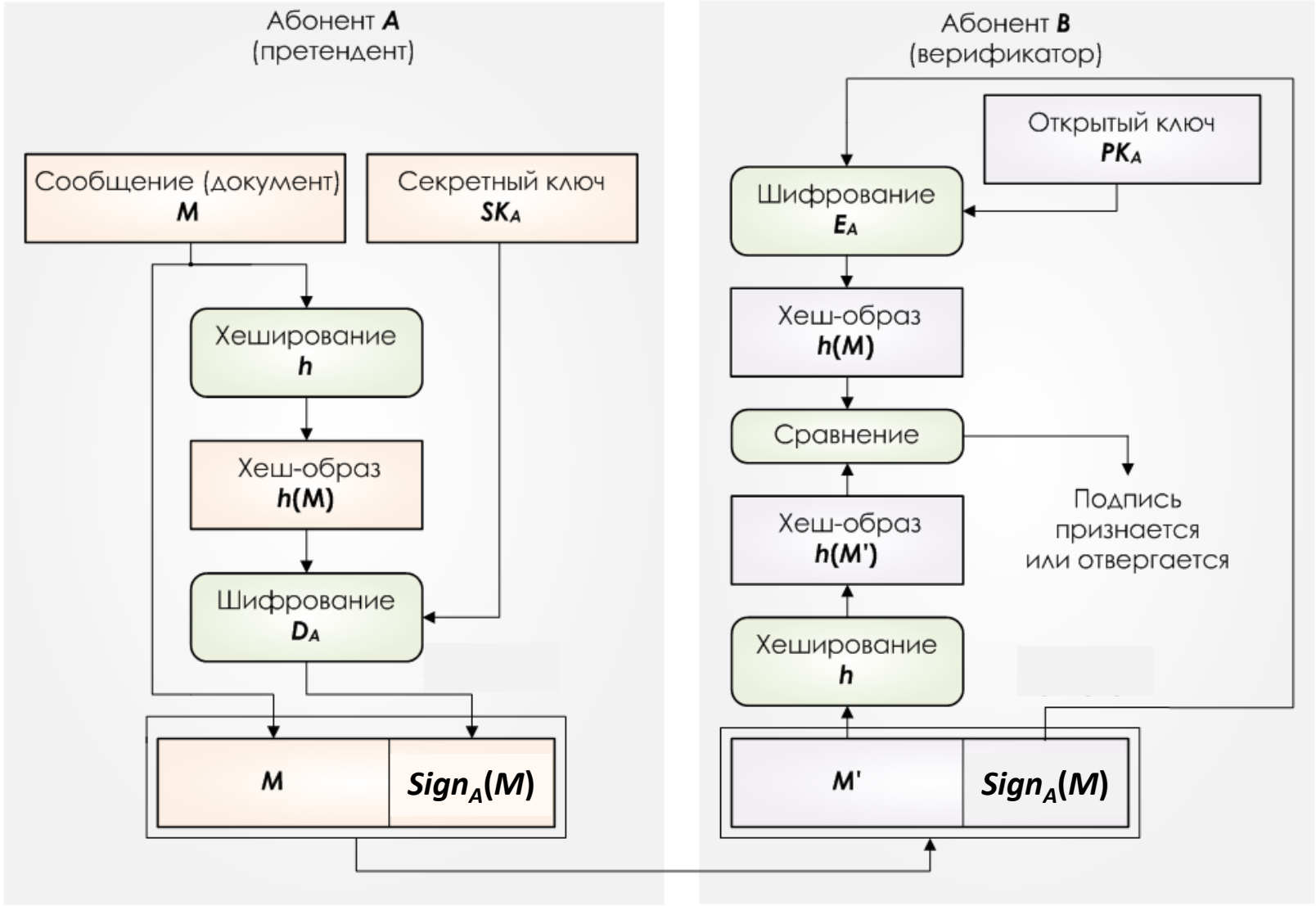
- При заданном значении M задача нахождения $h(M)$ должна быть вычислительно разрешима
- $h(M)$ должен зависеть от всех бит про-образа M и от их взаимного расположения
- Результат действия ХФ должен быть непредсказуем
- При заданном значении $h(M)$ задача нахождения M должна быть вычислительно неразрешимой (**pre-image resistance**)
- При заданных значениях $h(M)$ и первого прообраза M задача нахождения второго прообраза $M' \neq M$, такого, что $h(M') = h(M)$, должна быть вычислительно неразрешимой (**second pre-image resistance**)
- Задача нахождения коллизии ХФ, т.е. нахождение двух произвольных сообщений M_1 и M_2, таких, что $M_1 \neq M_2$, а $h(M_1) = h(M_2)$, должна быть вычислительно неразрешимой (**collision resistance**)



Задачи: *а* – нахождение прообраза; *б* – нахождение второго прообраза; *в* – нахождение коллизии

Протокол классической ЭП

$Sign_A(M)$



Протокол электронной подписи (ЭП)

- Наиболее стойкими являются схемы ЭП, стойкие против самой слабой из угроз на основе самой сильной из атак

- Стойкие схемы ЭП существуют тогда и только тогда, когда существуют односторонние функции

Протокол электронной подписи (ЭП)

- Наиболее стойкими являются схемы ЭП, стойкие против самой слабой из угроз на основе самой сильной из атак

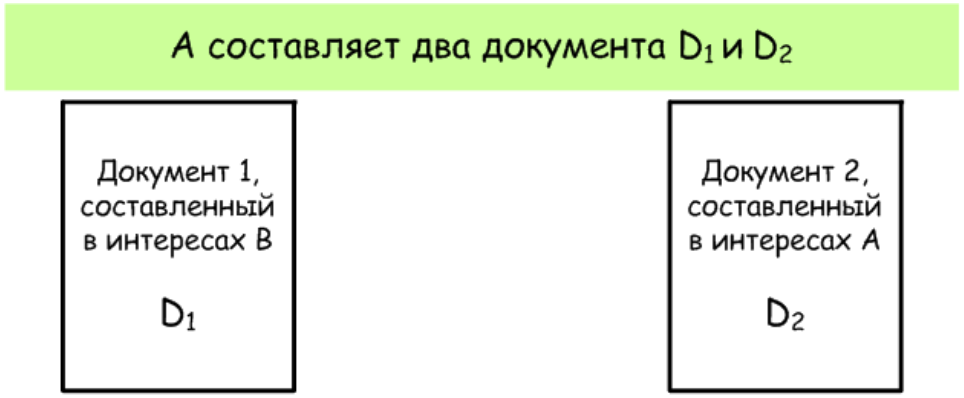
- Стойкие схемы ЭП существуют тогда и только тогда, когда существуют односторонние функции

Характеристика	Рукописная подпись	ЭП
Возможность подделки, кто может выявить факт подделки	Да, специалист-графолог	Да, специалист-криптолог
Возможность копирования подписанного документа	Нет	Да
Возможность раздельного хранения или пересылки документа и подписи	Нет	Да

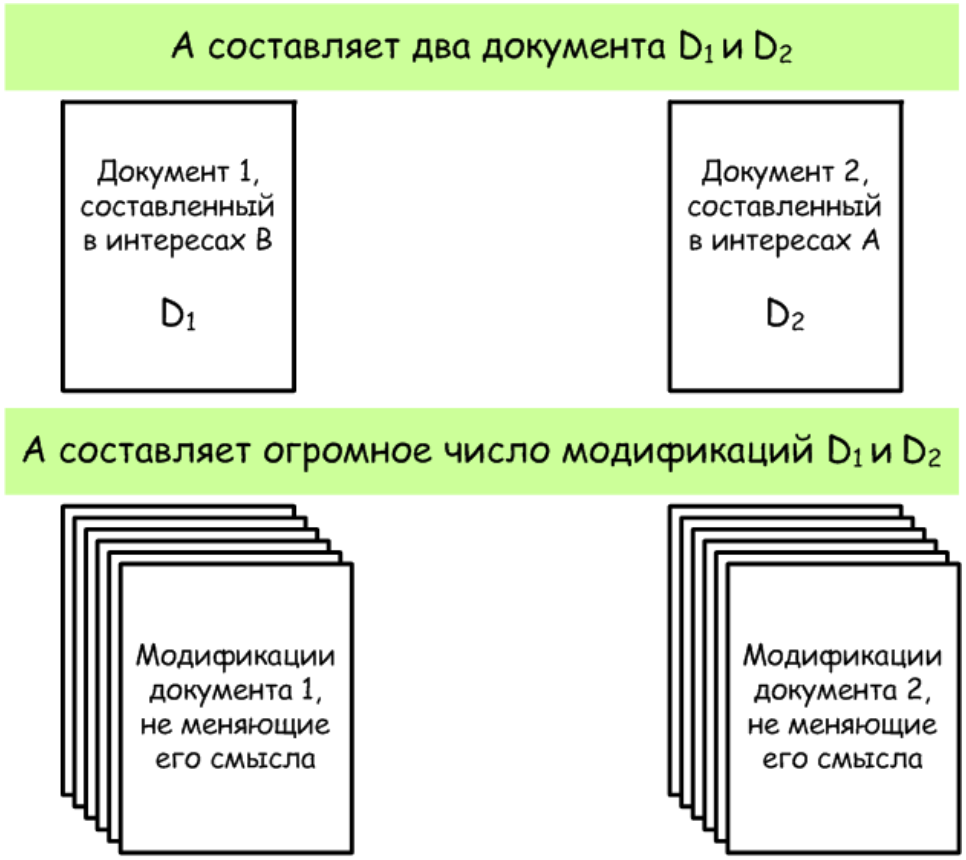
Ввод в схему электронной подписи
операции хеширования
повышает или понижает
безопасность протокола в целом?

Атака на схему ЭП, основанная на парадоксе дней рождения

Атака на схему ЭП, основанная на парадоксе дней рождения

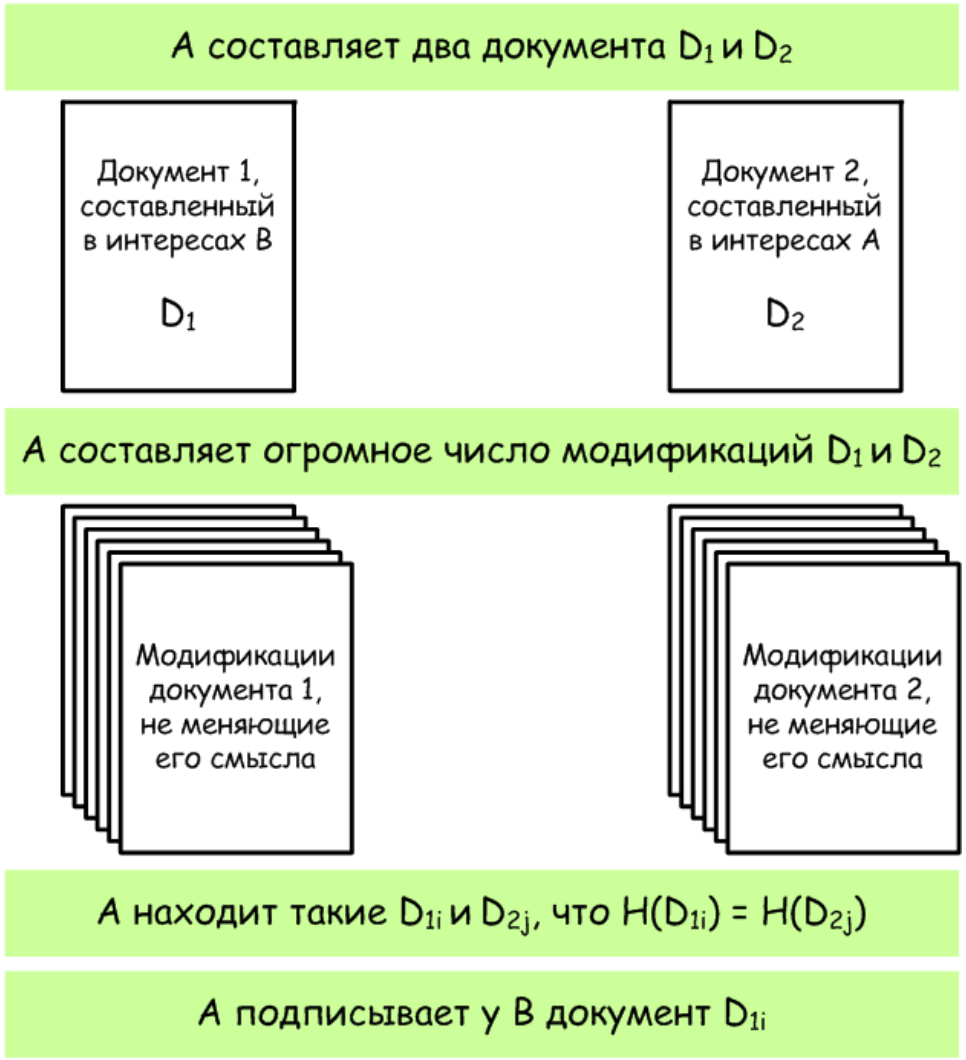


Атака на схему ЭП, основанная на парадоксе дней рождения

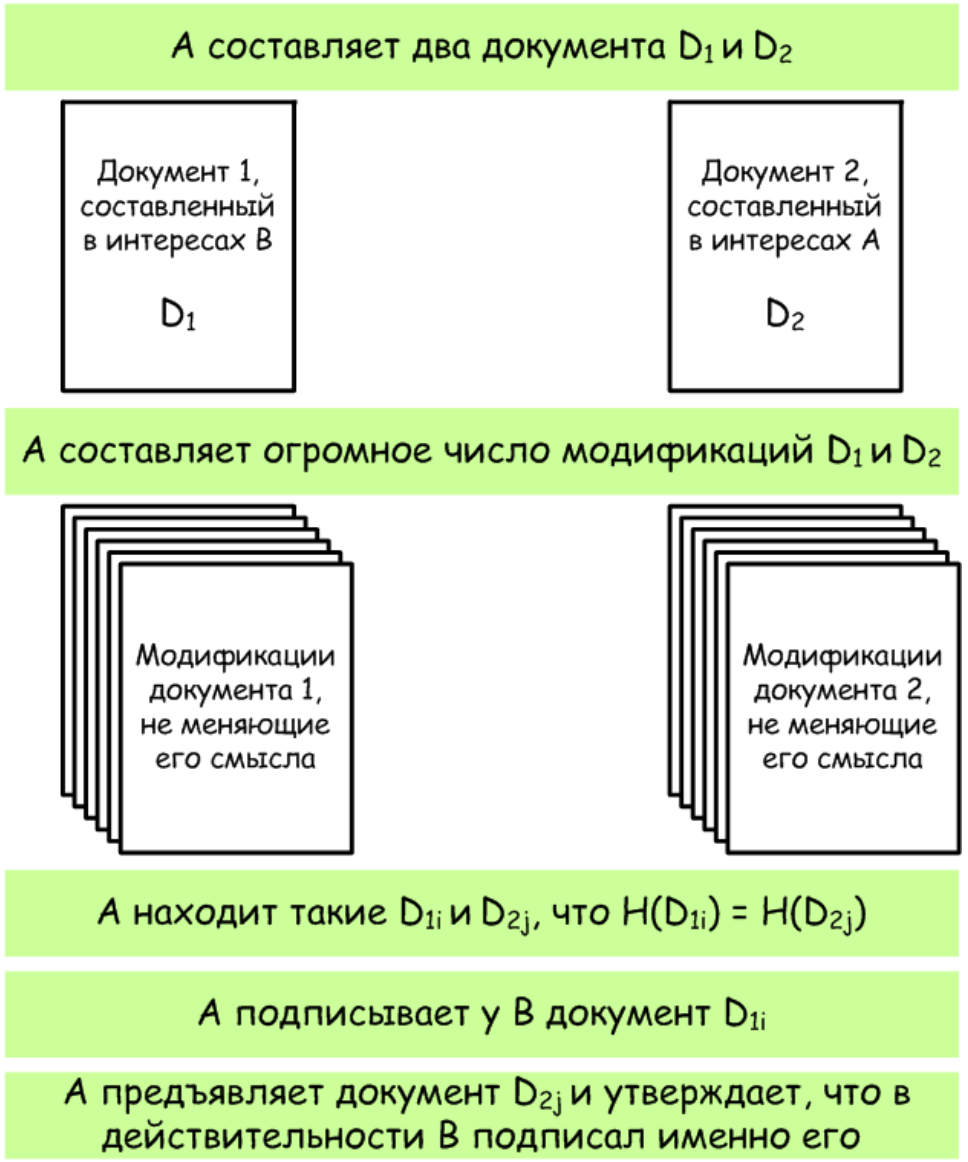


Атака на схему ЭП, основанная на парадоксе дней рождения

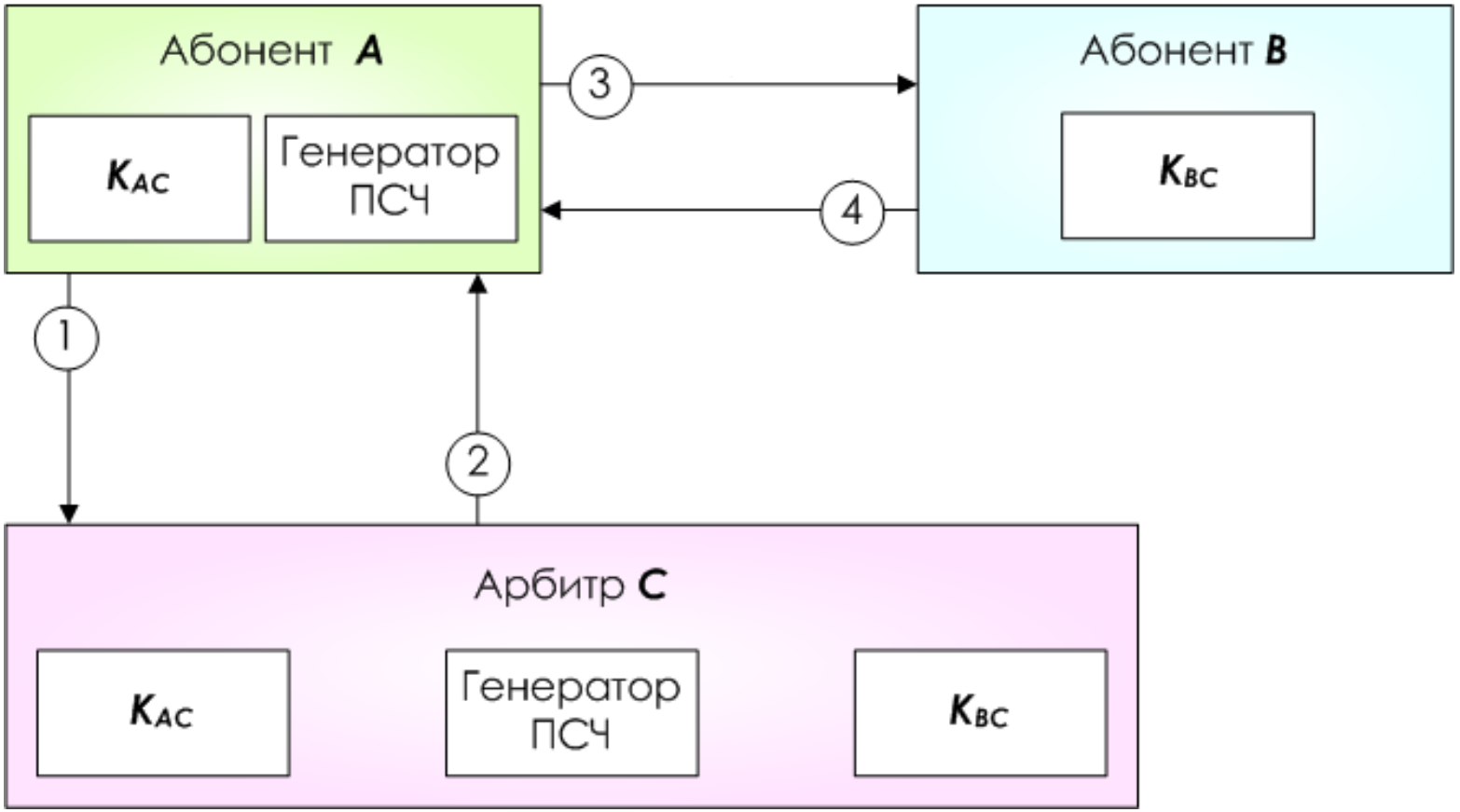
Атака на схему ЭП, основанная на парадоксе дней рождения



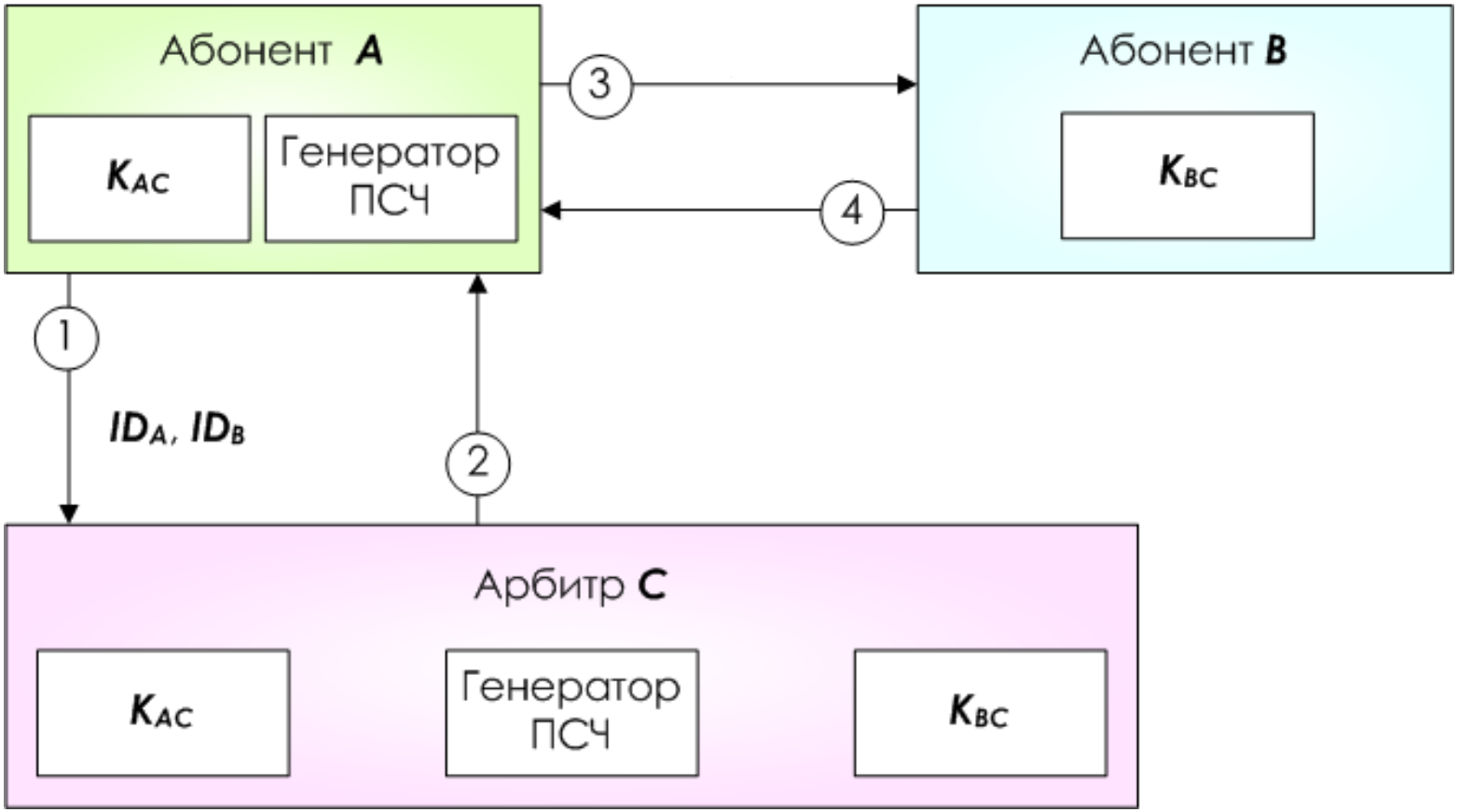
Атака на схему ЭП, основанная на парадоксе дней рождения



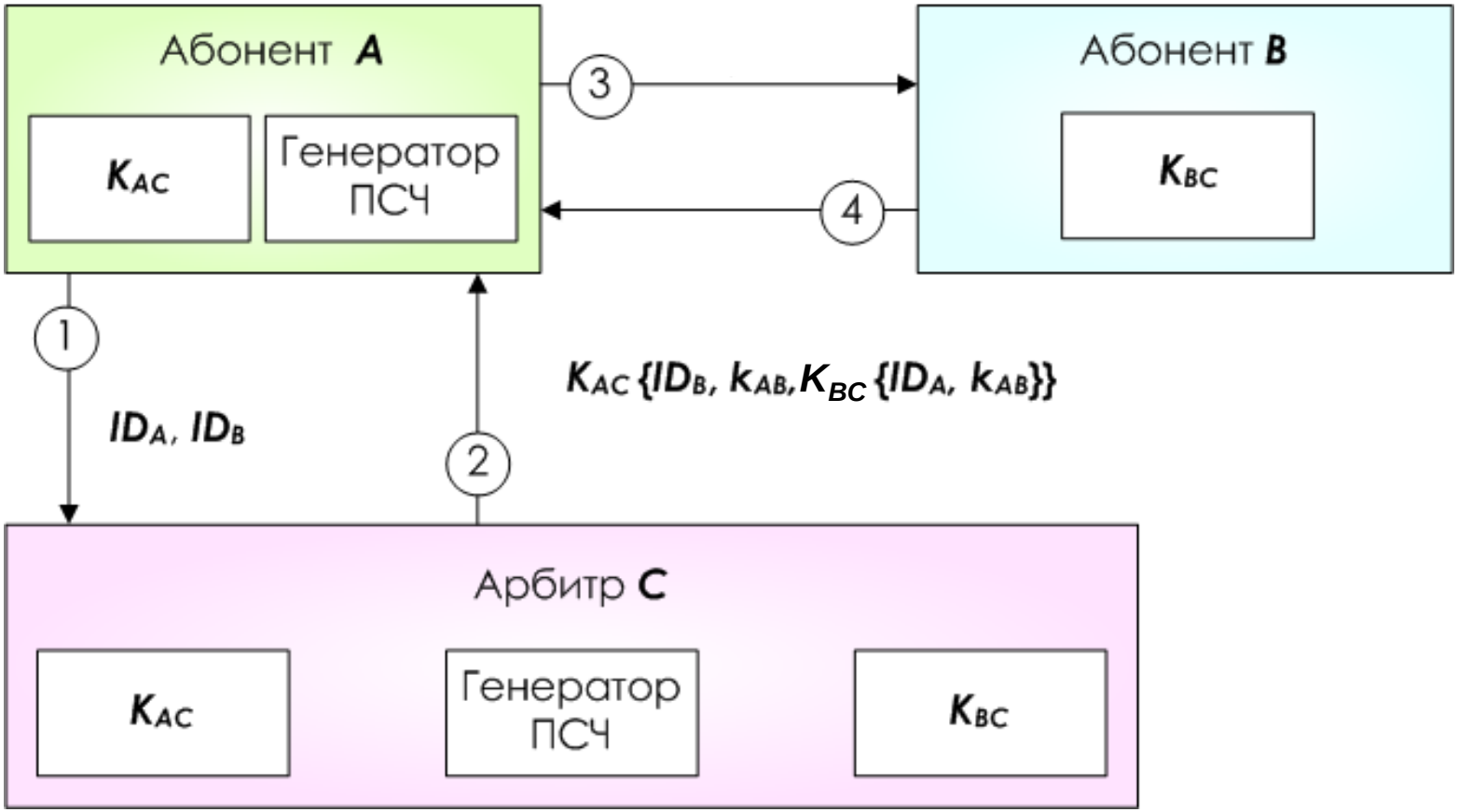
Протокол аутентификации Нидхэма-Шредера



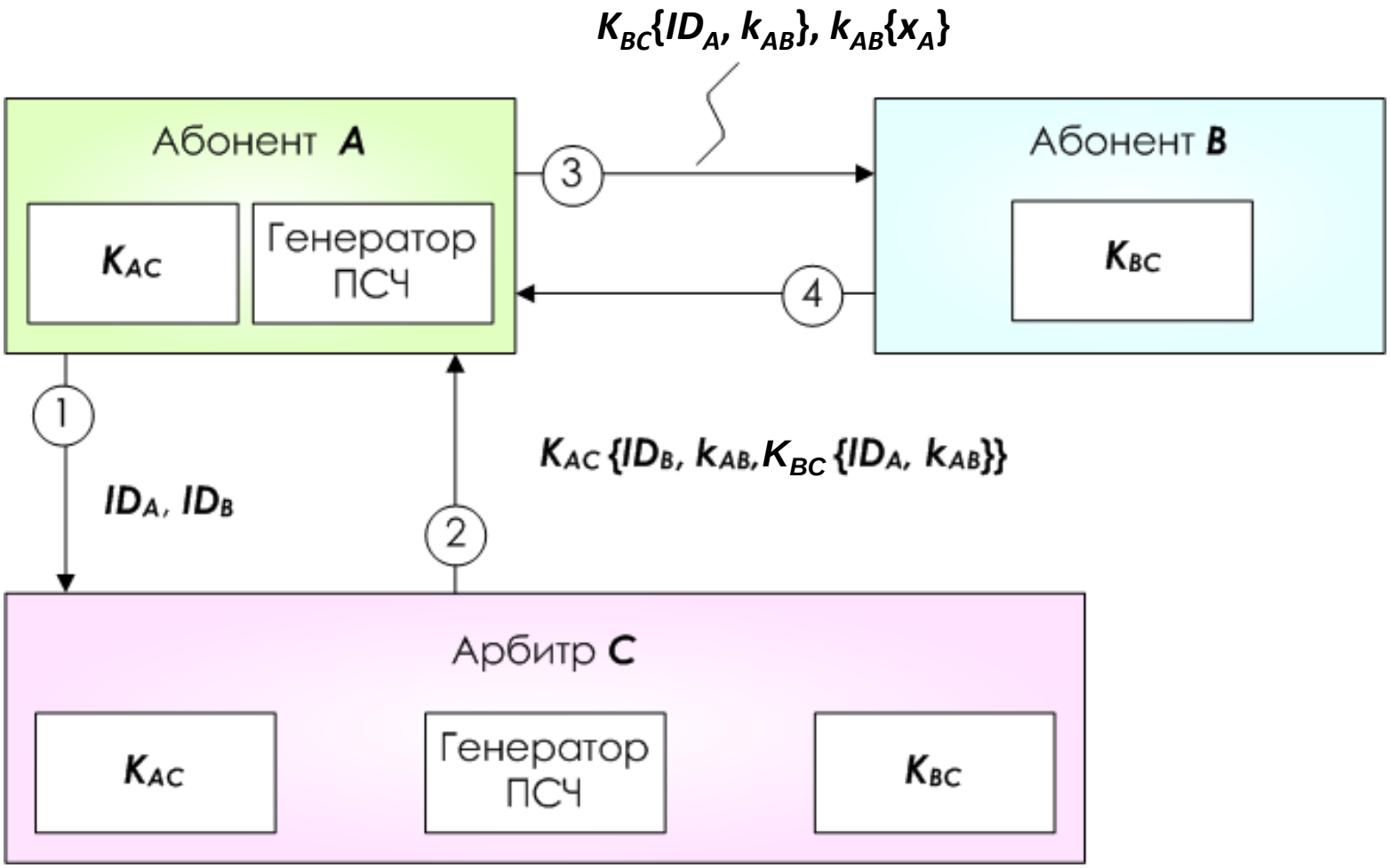
Протокол аутентификации Нидхэма-Шредера



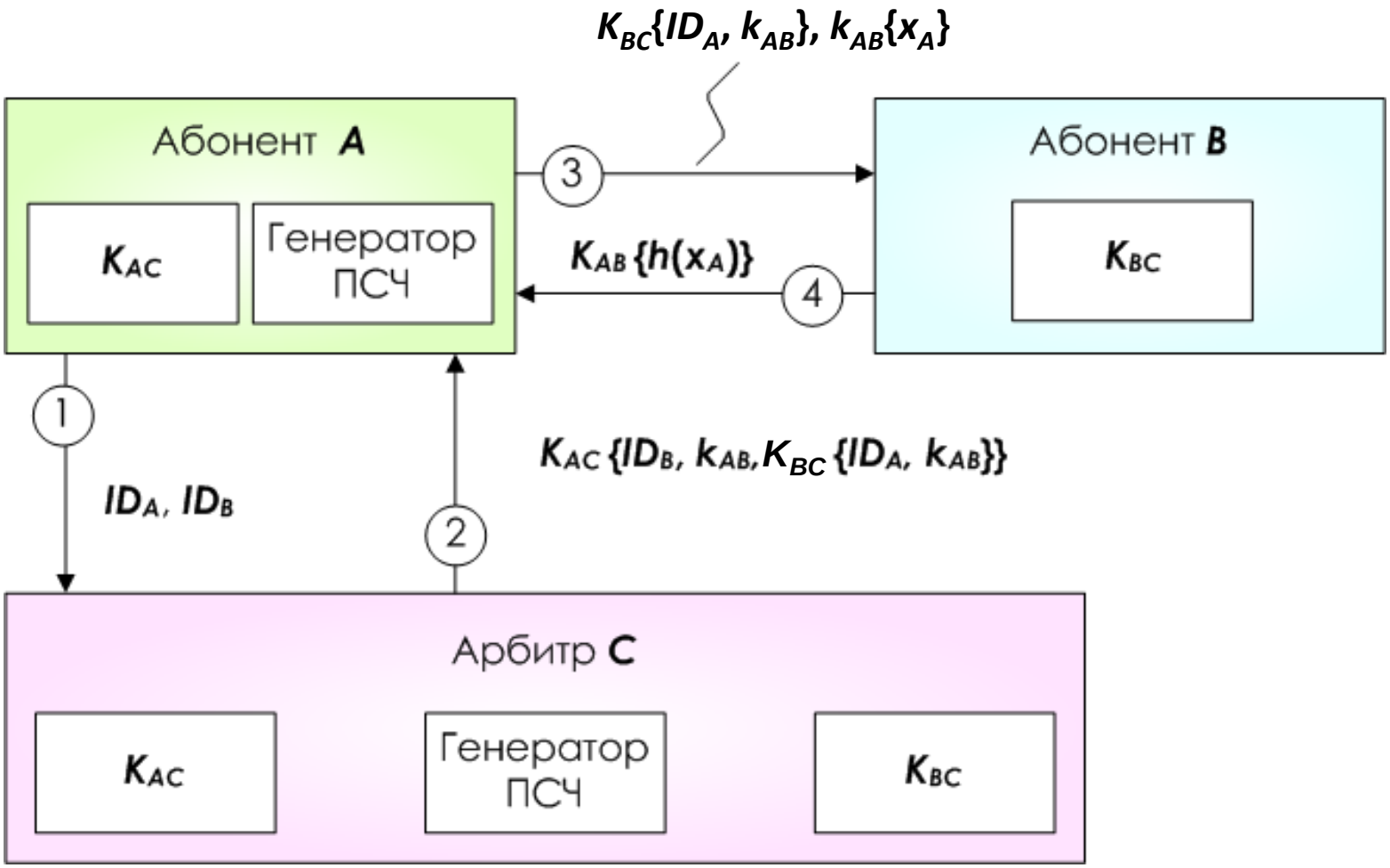
Протокол аутентификации Нидхэма-Шредера



Протокол аутентификации Нидхэма-Шредера



Протокол аутентификации Нидхэма-Шредера



Протокол аутентификации Нидхэма-Шредера

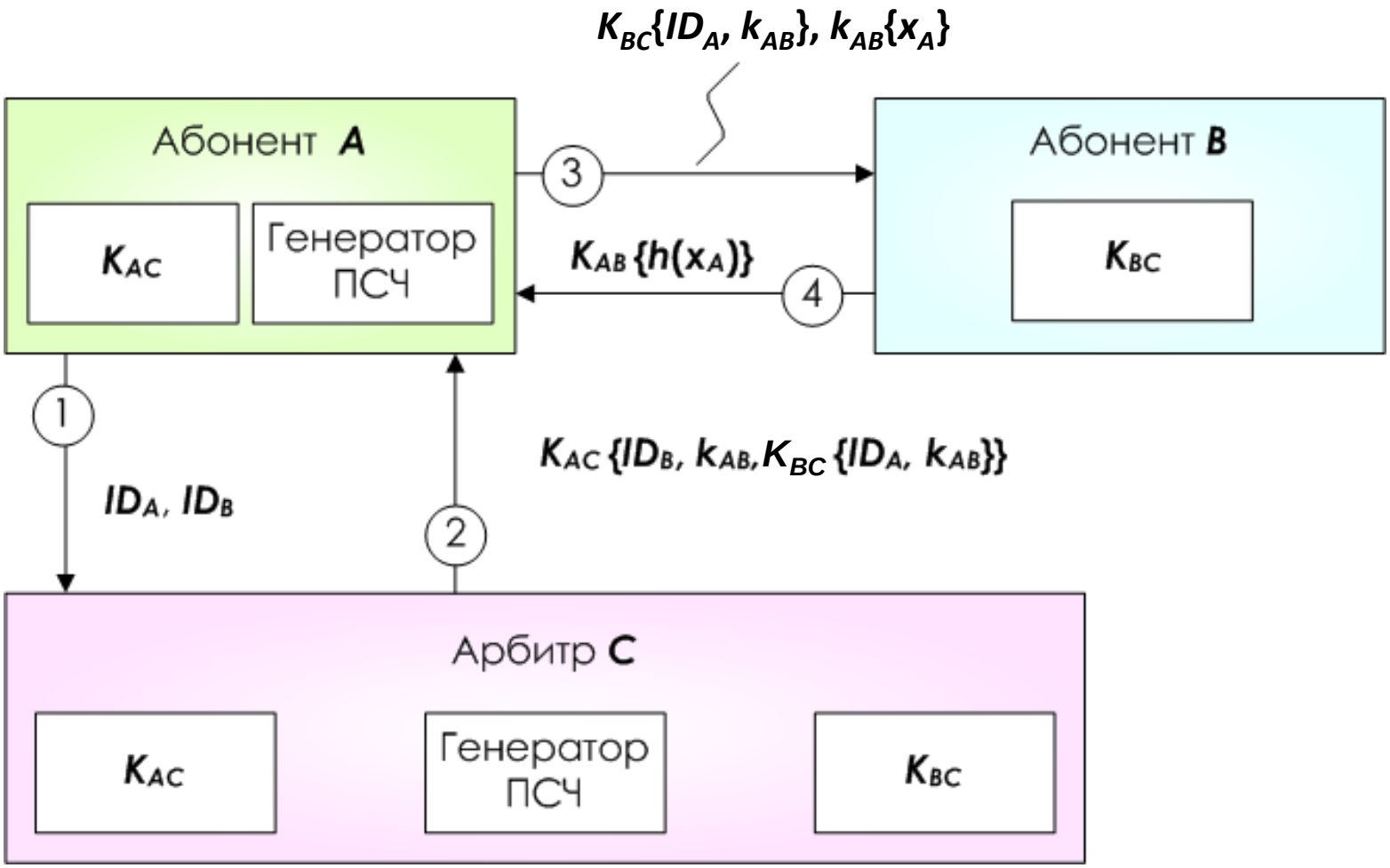


Схема Kerberos

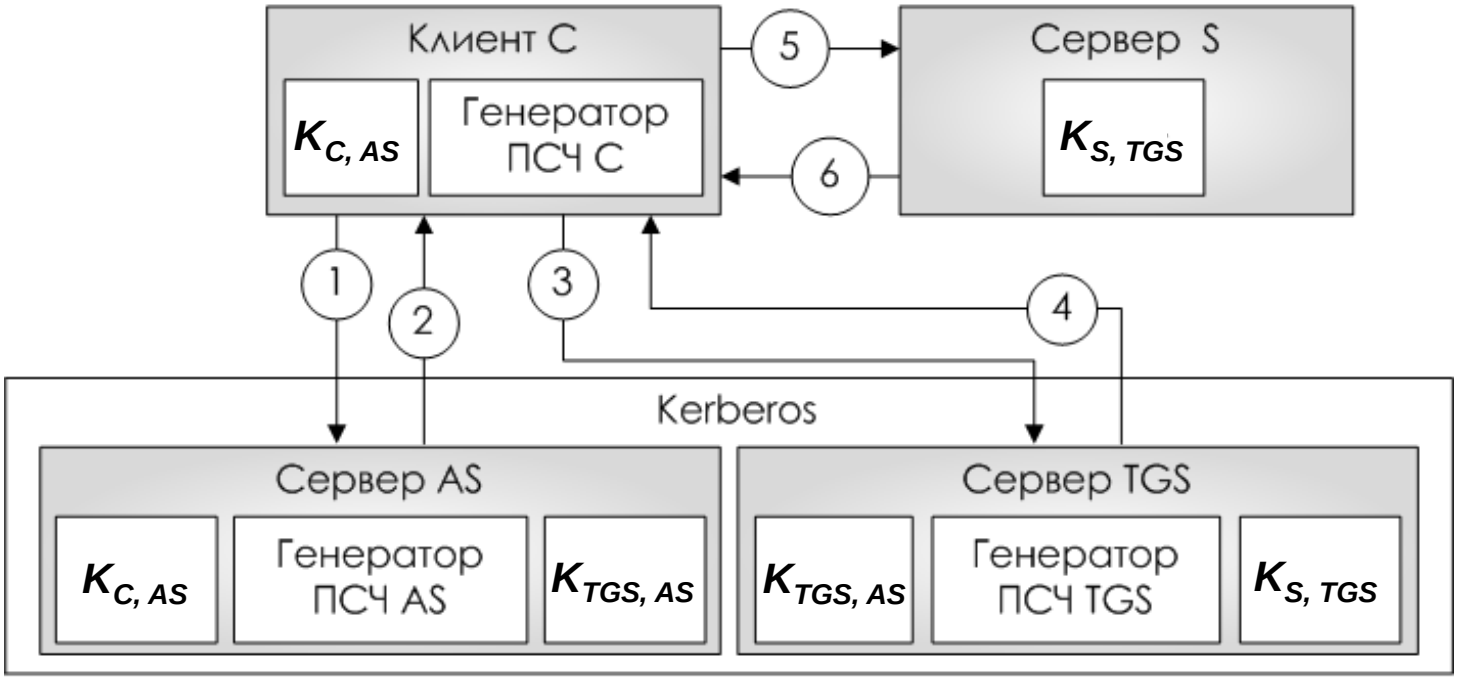
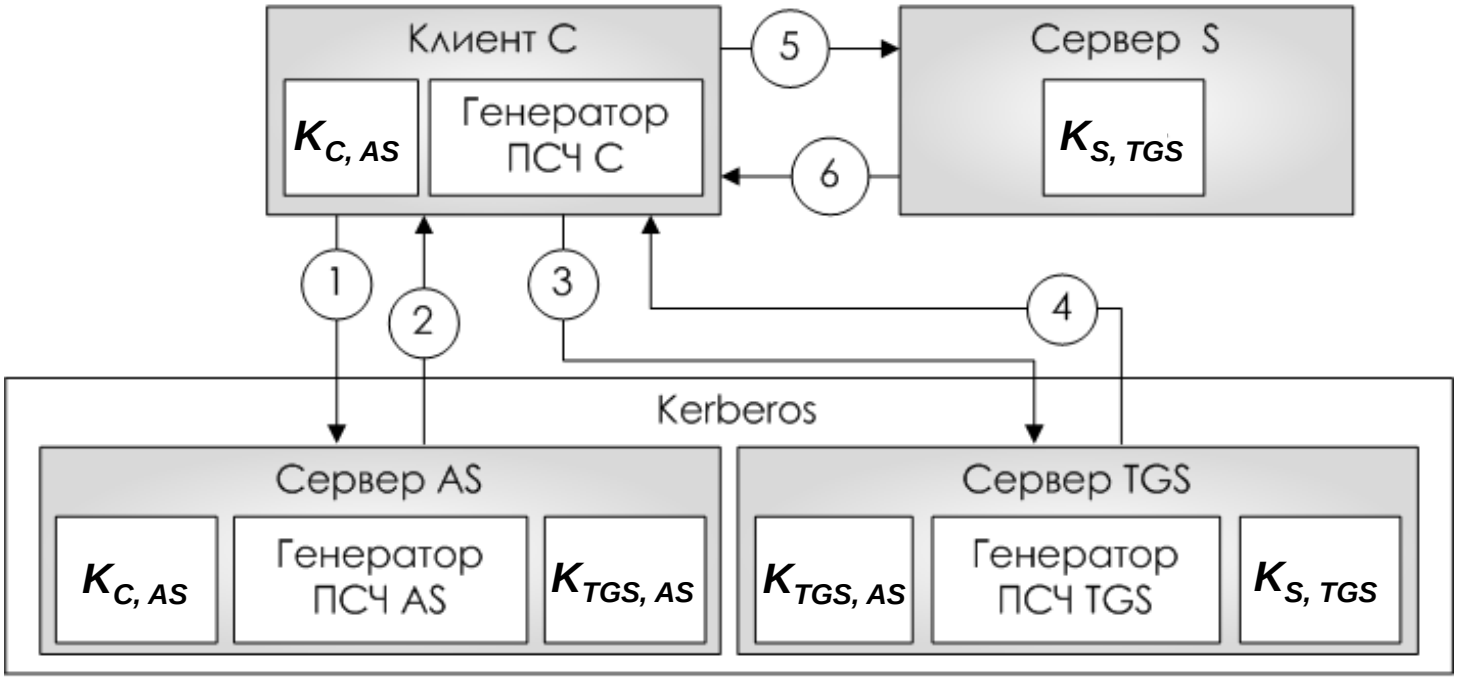


Схема Kerberos



Метки: *tl* – время жизни ключа, *ts* – время отправки сообщения

Схема Kerberos

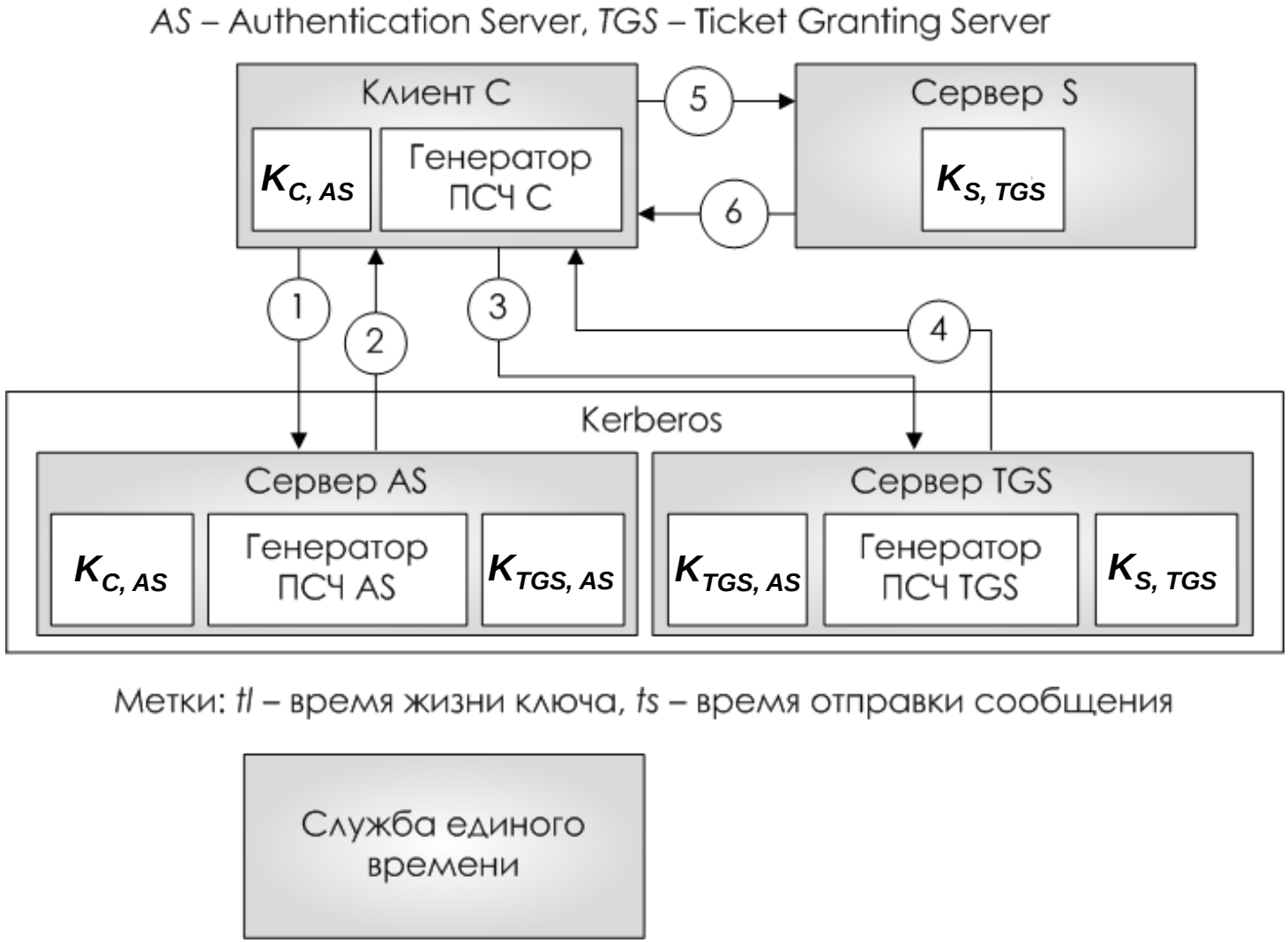


Схема Kerberos

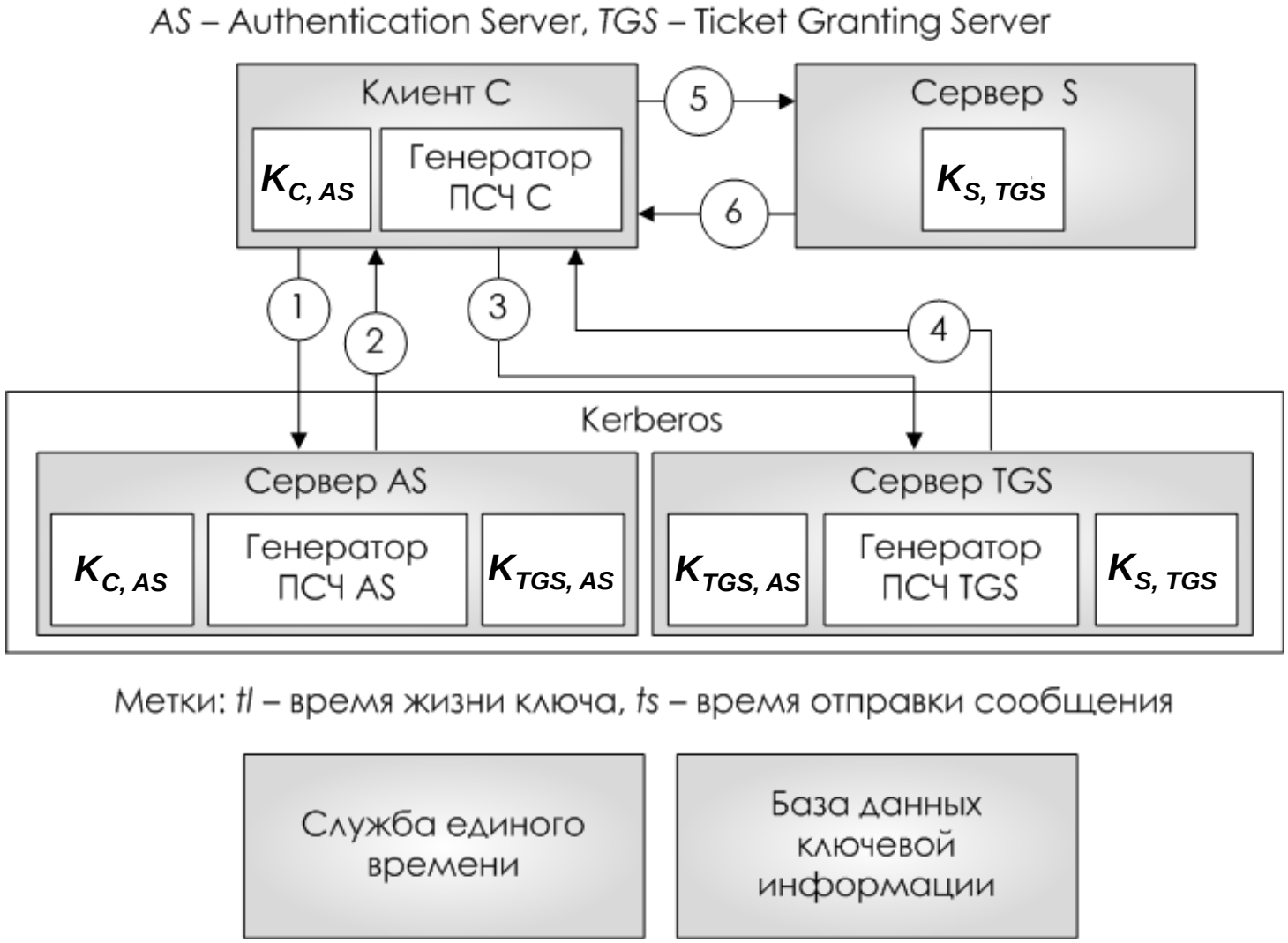
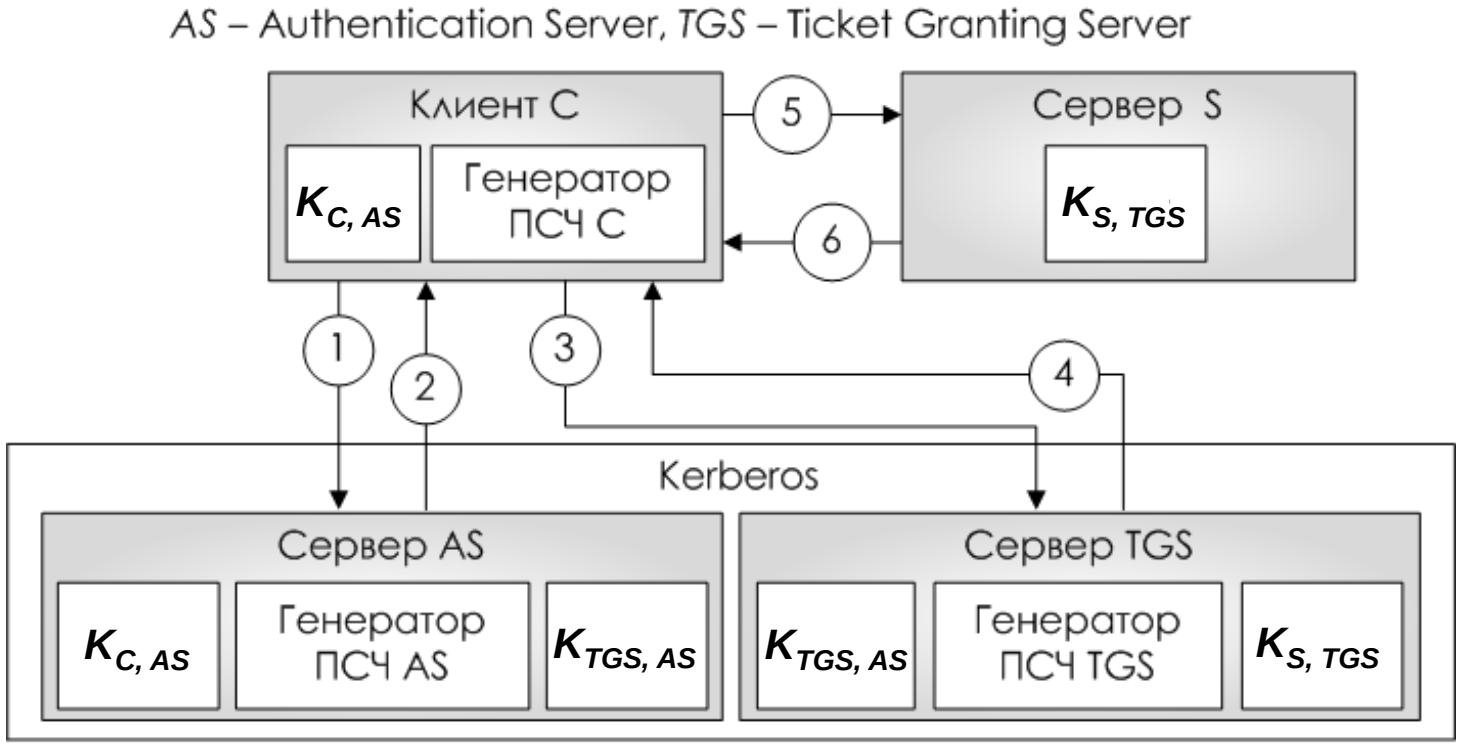


Схема Kerberos



Участников стало больше, пересылаемых сообщений стало больше ⇨ стойкость ⇩ ???

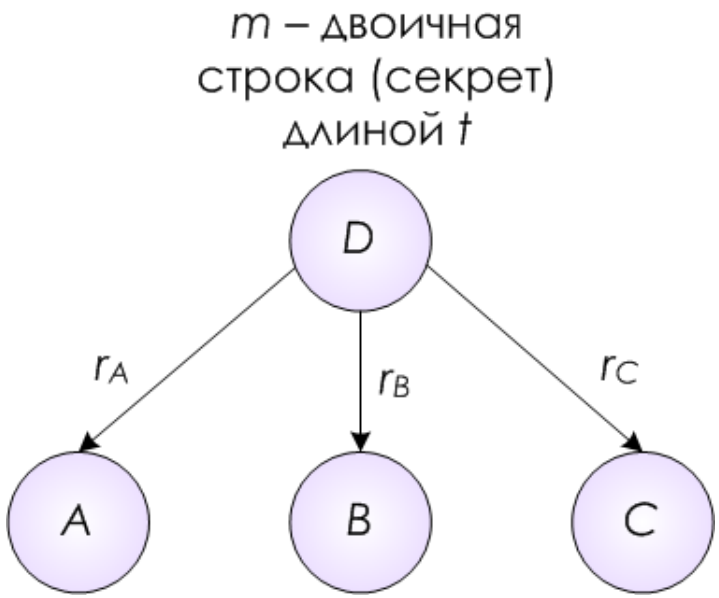
Протокол разделения секрета

- Ограничение доступа
- Разграничение доступа
- Разделение доступа

Протокол разделения секрета

Распределение долей секрета

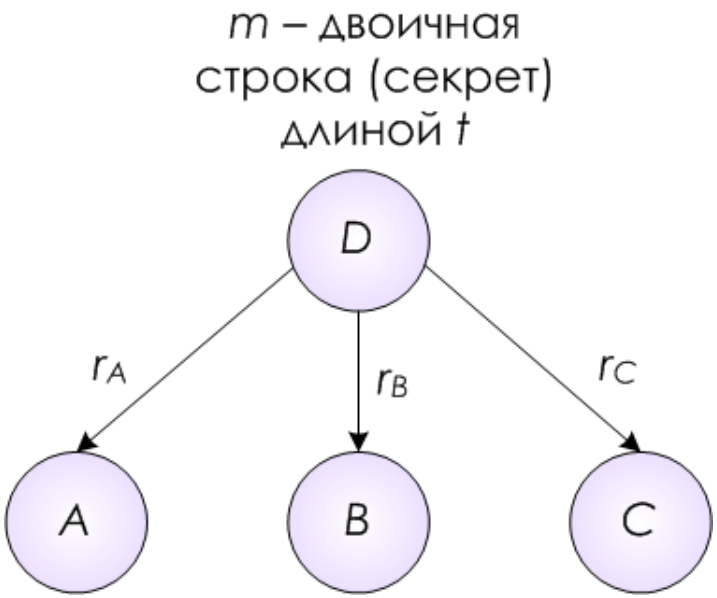
- D: r_A и r_B – случайные строки длиной t
- D: $r_C = m \oplus r_A \oplus r_B$
- D: $r_A \rightarrow A$, $r_B \rightarrow B$, $r_C \rightarrow C$



Протокол разделения секрета

Распределение долей секрета

- D: r_A и r_B – случайные строки длиной t
- D: $r_C = m \oplus r_A \oplus r_B$
- D: $r_A \rightarrow A$, $r_B \rightarrow B$, $r_C \rightarrow C$



Восстановление секрета

- A, B и C предъявляют свои доли секрета r_A, r_B и r_C и вычисляют $m = r_A \oplus r_B \oplus r_C$

Протокол подбрасывания монеты. Схема Блюма

Физическая интерпретация протокола

- Абонент B выбирает случайный бит b, записывает его на листе бумаги, запирает этот лист в ящик, оставляя ключ у себя, и посылает ящик абоненту A

Протокол подбрасывания монеты. Схема Блюма

Физическая интерпретация протокола

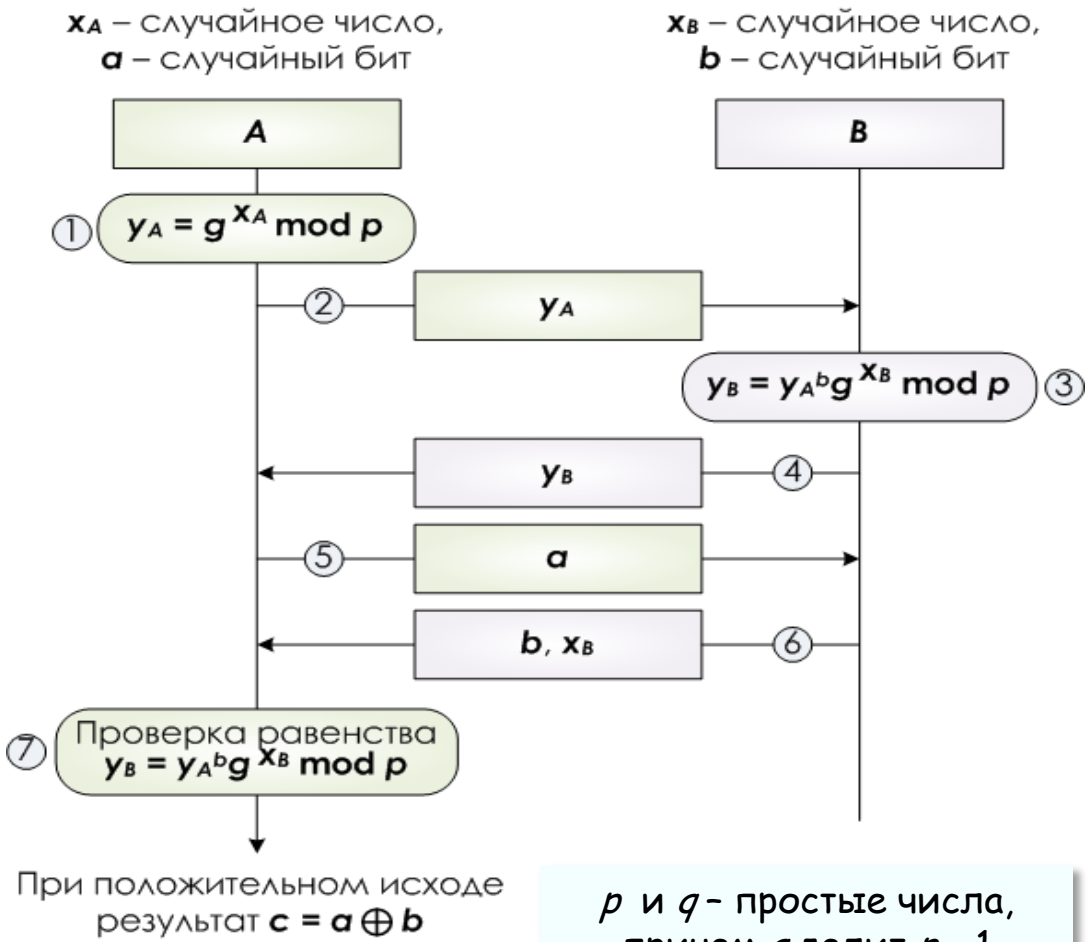
- Абонент B выбирает случайный бит b, записывает его на листе бумаги, запирает этот лист в ящик, оставляя ключ у себя, и посылает ящик абоненту A
- Получив запертый ящик, абонент A не может добраться до его содержимого. Он выбирает случайный бит a и посылает его абоненту B. В ответ B посылает A ключ от ящика, а затем определяет исход подбрасывания монеты $c = a \oplus b$

Протокол подбрасывания монеты. Схема Блюма

Физическая интерпретация протокола

- Абонент B выбирает случайный бит b, записывает его на листе бумаги, запирает этот лист в ящик, оставляя ключ у себя, и посылает ящик абоненту A
- Получив запертый ящик, абонент A не может добраться до его содержимого. Он выбирает случайный бит a и посылает его абоненту B. В ответ B посылает A ключ от ящика, а затем определяет исход подбрасывания монеты $c = a \oplus b$
- Абонент A, получив ключ, отпирает ящик, читает b и точно таким же образом узнает c

Протокол подбрасывания монеты. Схема Блюма



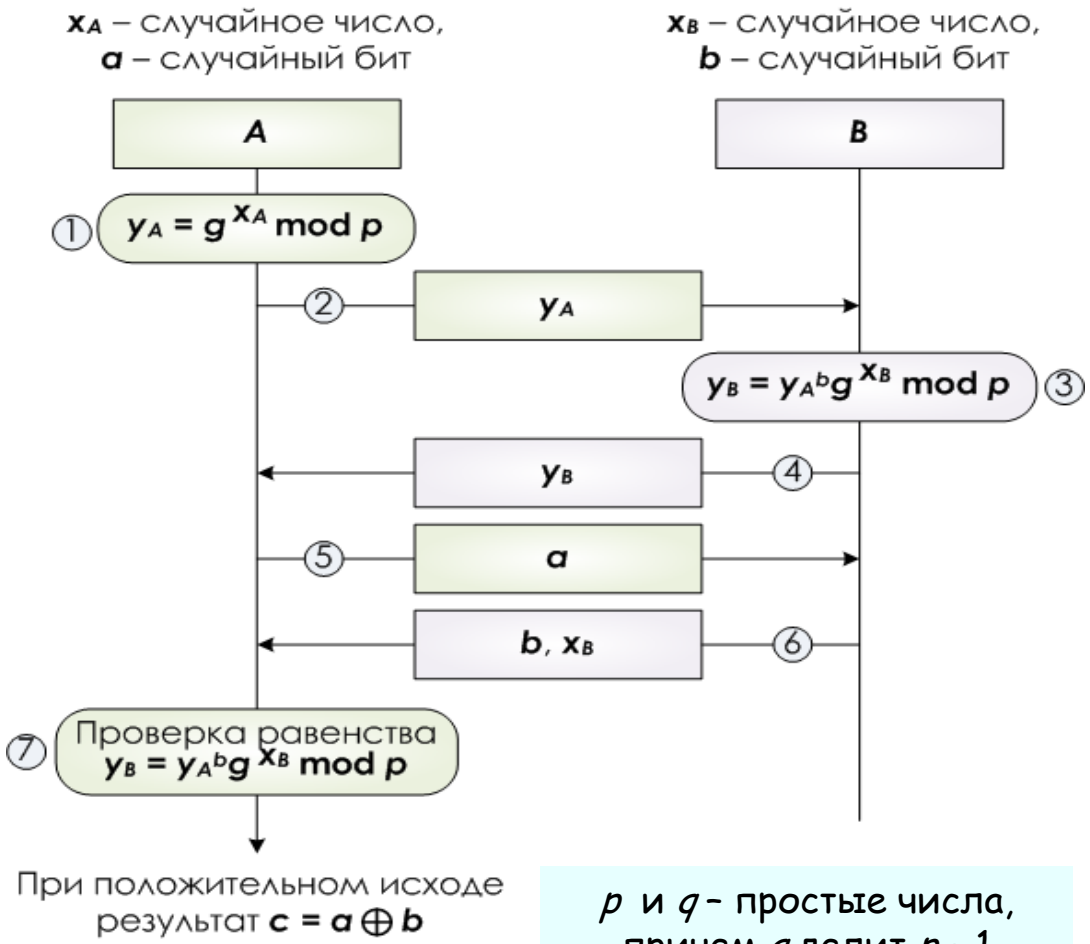
p и q – простые числа, причем q делит $p - 1$

$g \in Z_p$, $g^q \equiv 1 \bmod p$, $g \neq 1$

Физическая интерпретация протокола

- Абонент B выбирает случайный бит b, записывает его на листе бумаги, запирает этот лист в ящик (y_B – суть криптографический аналог этого ящика), оставляя ключ (x_B) у себя, и посылает ящик абоненту A
- Получив запертый ящик, абонент A не может добраться до его содержимого. Он выбирает случайный бит a и посылает его абоненту B. В ответ B посылает A ключ от ящика, а затем определяет исход подбрасывания монеты $c = a \oplus b$
- Абонент A, получив ключ, отпирает ящик, читает b и точно таким же образом узнает c

Протокол подбрасывания монеты. Схема Блюма



p и q – простые числа, причем q делит $p - 1$

$g \in Z_p$, $g^q \equiv 1 \bmod p$, $g \neq 1$

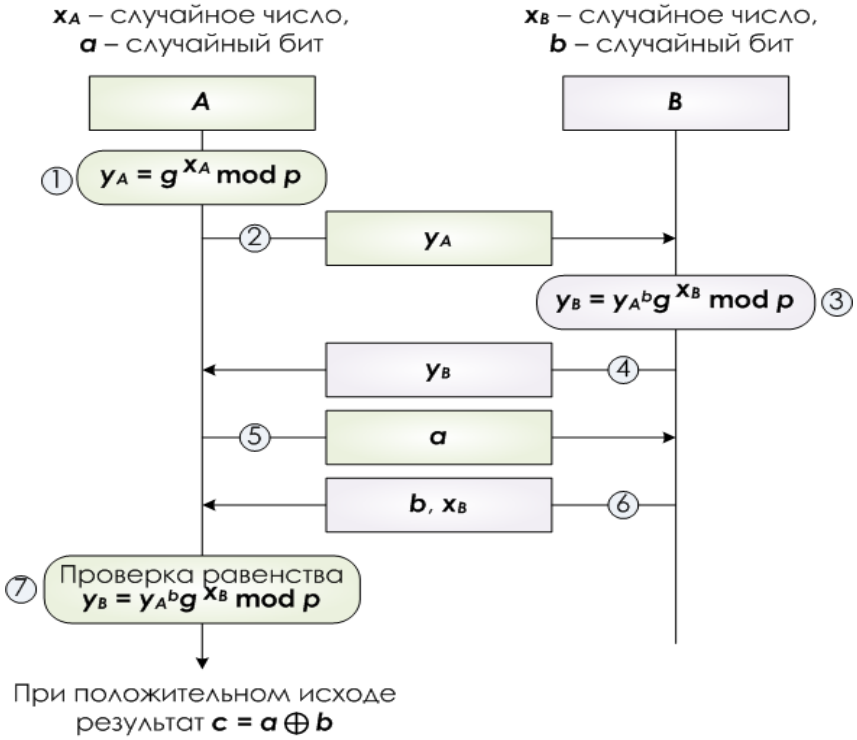
Физическая интерпретация протокола

- Абонент B выбирает случайный бит b, записывает его на листе бумаги, запирает этот лист в ящик (y_B – суть криптографический аналог этого ящика), оставляя ключ (x_B) у себя, и посылает ящик абоненту A
- Получив запертый ящик, абонент A не может добраться до его содержимого. Он выбирает случайный бит a и посылает его абоненту B. В ответ B посылает A ключ от ящика, а затем определяет исход подбрасывания монеты $c = a \oplus b$
- Абонент A, получив ключ, отпирает ящик, читает b и точно таким же образом узнает c

A: $x_A = 4$, $a = 1$
B: $x_B = 7$, $b = 0$

1) A: $y_A = 2^4 \bmod 31 = 16$
2) A: $y_A = 16 \rightarrow B$
3) B: $y_B = 16^0 \cdot 2^7 \bmod 31 = 128 \bmod 31 = 4$
4) B: $y_B = 4 \rightarrow A$
5) A: $a = 1 \rightarrow B$
6) B: $b = 0$, $x_B = 7 \rightarrow A$
7) A: проверка равенства
   $4 = 16^0 \cdot 2^7 \bmod 31 \rightarrow 4 = 4$
8) A, B: $c = 1 \oplus 0 = 1$

1) A: $y_A = 2^4 \bmod 31 = 16$
2) A: $y_A = 16 \rightarrow B$
3) B: $y_B = 16^0 \cdot 2^7 \bmod 31 = 128 \bmod 31 = 4$
4) B: $y_B = 4 \rightarrow A$
5) A: $a = 1 \rightarrow B$
6) B: $b' = 1$, $x_B = 7 \rightarrow A$
7) A: проверка равенства
   $4 = 16^1 \cdot 2^7 \bmod 31 \rightarrow 16 \cdot 4 \bmod 31 = 2 \neq 4$



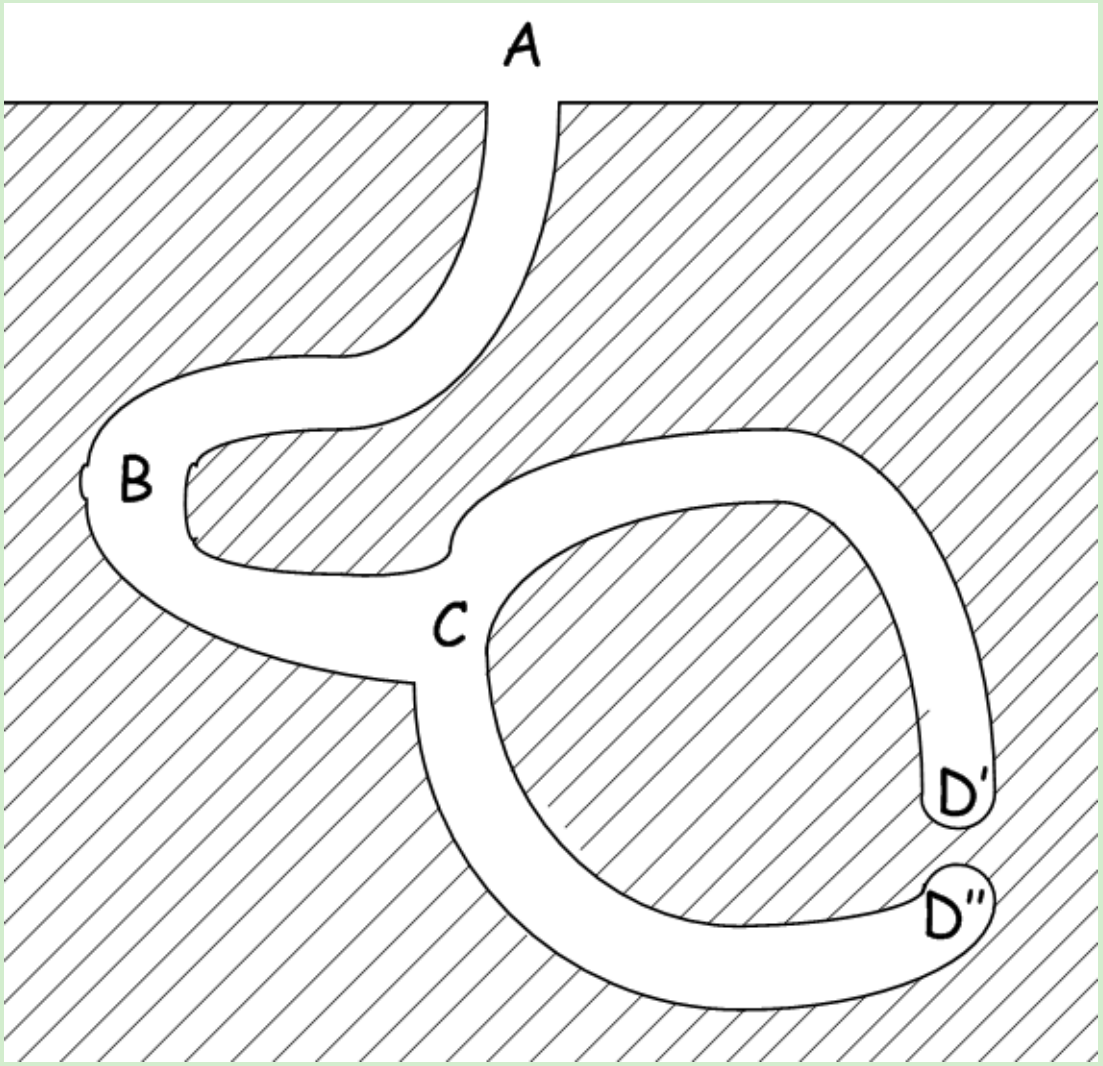
p и q – простые числа,
причем q делит p – 1
$g \in Z_p$, $g^q \equiv 1 \bmod p$, $g \neq 1$

p = 31, q = 5 → q делит p – 1
$g = 2$, $2^5 = 32 \rightarrow 2^5 \equiv 1 \bmod 31$

Пещера нулевого знания Б. Шнайера

Доказывающий

P

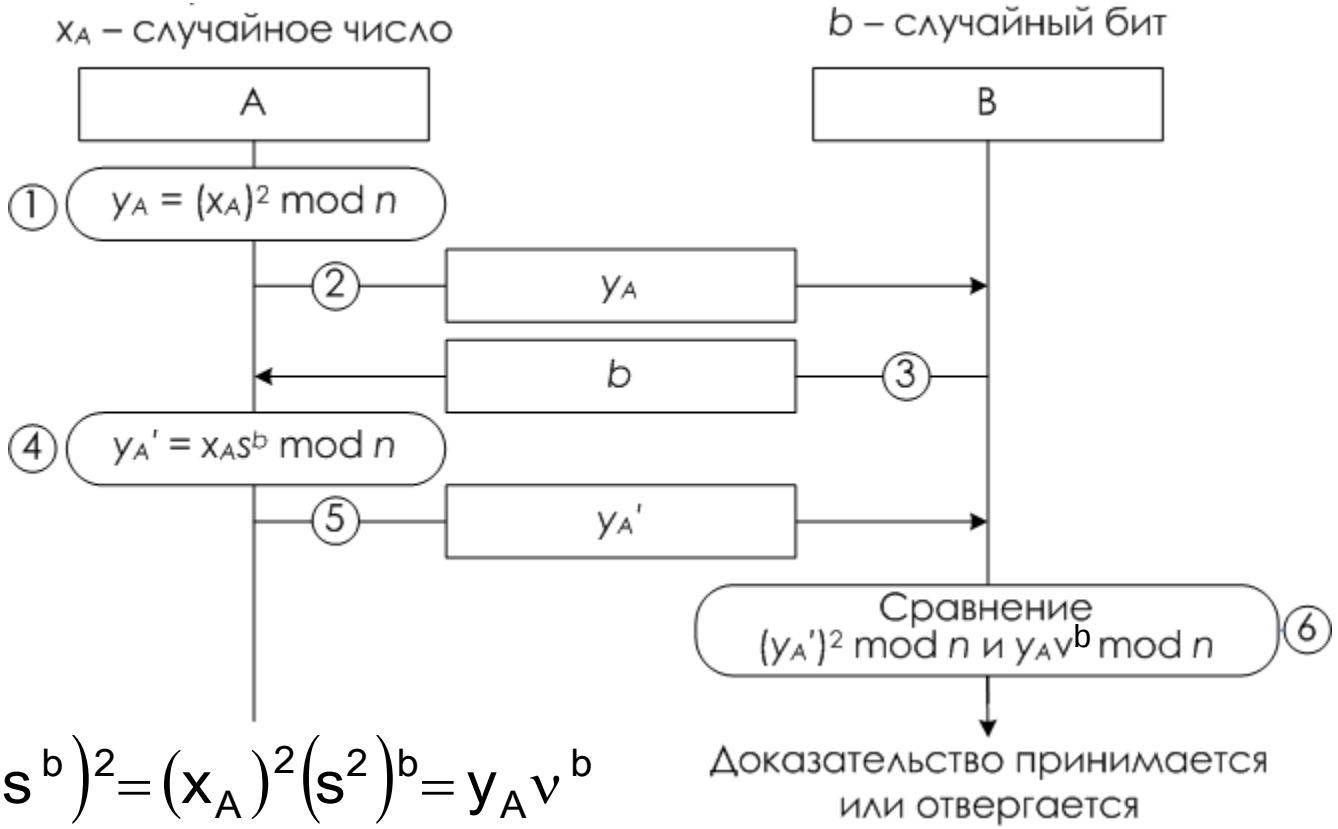


Проверяющий

V

Протокол Фиата-Шамира. Одна итерация

- Доверенный третий участник протокола выбирает два больших простых числа p и q, затем вычисляет n = pq
- Абонент A выбирает случайное число $s \in Z_n$, вычисляет $v = s^2 \bmod n$. A хранит s в качестве своего секретного ключа и объявляет (v, n) своим открытым ключом

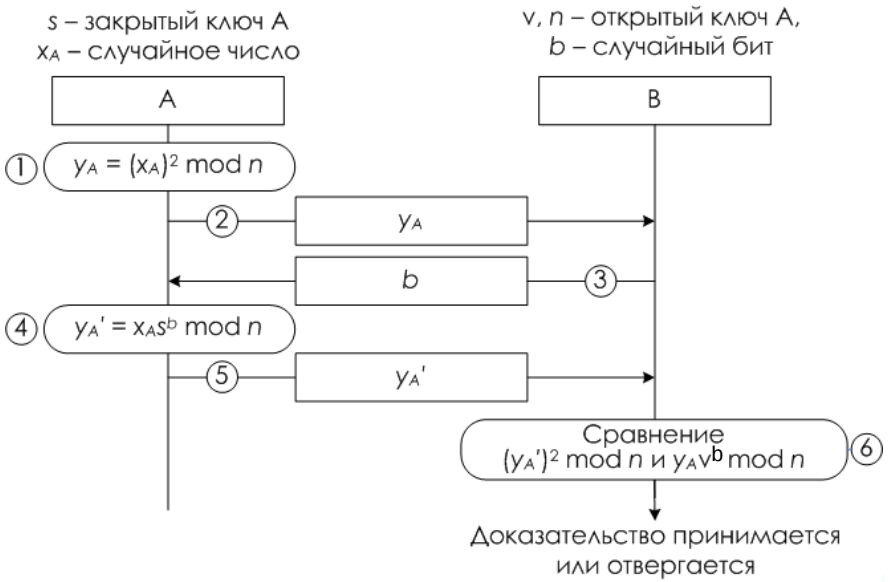


$$y'^{2}_{A} = \left(x_A s^{b}\right)^2 = \left(x_A\right)^2 \left(s^2\right)^b = y_A v^{b}$$

A: $x_A = 9$
B: b = 1

1) A: $y_A = 9^2 \bmod 33 = 81 \bmod 33 = 15$
2) A: $y_A = 15 \rightarrow B$
3) B: $b = 1 \rightarrow A$
4) A: $y'_A = 9 \cdot 7^1 \bmod 33 = 30$
5) A: $Y'_A = 30 \rightarrow B$
6) B: проверка равенства
   $30^2 \bmod 33 = 15 \cdot 16^1 \bmod 33 \rightarrow 9 = 9$
   Доказательство принимается

1) A: $y_A = 9^2 \bmod 33 = 81 \bmod 33 = 15$
2) A: $y_A = 15 \rightarrow B$
3) B: $b = 1 \rightarrow A$
4) A: $y'_A = 8$
5) A: $Y'_A = 8 \rightarrow B$
6) B: проверка равенства
   $8^2 \bmod 33 = 15 \cdot 16^1 \bmod 33 \rightarrow 31 \neq 9$
   Доказательство не принимается



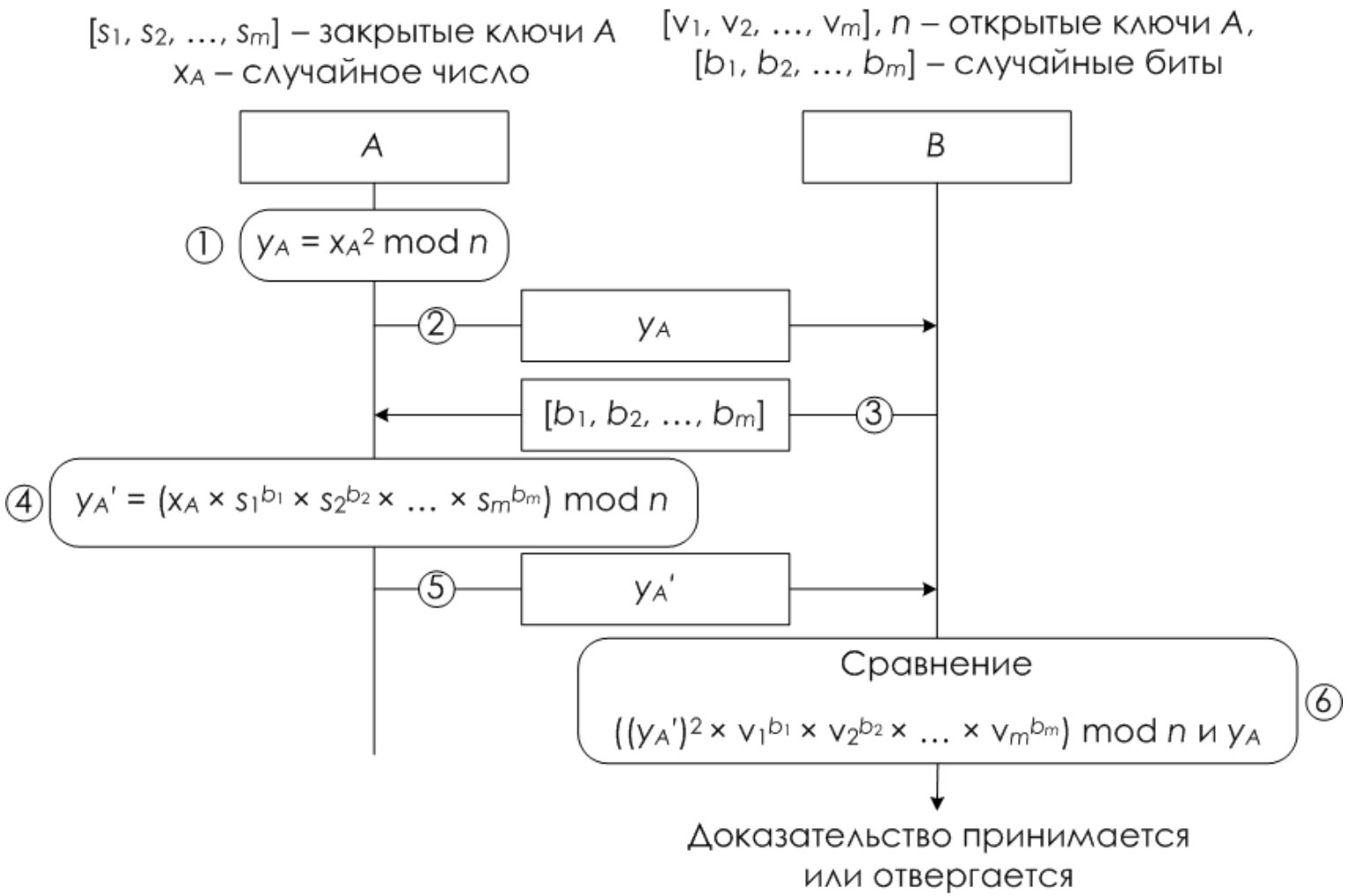
- Доверенный третий участник протокола bвыбирает два больших простых числа p и q, затем вычисляет n = pq
- Абонент A выбирает случайное число $s \in Z_n$, вычисляет $v = s^2 \bmod n$. A хранит s в качестве своего секретного ключа и объявляет (v, n) своим открытым ключом

p = 3, q = 11 → n = 33
A: $s = 7 \rightarrow v = 7^2 \bmod 33 = 16$
s = 7– Secret Key
(v, n) = (16, 33) – Public Key

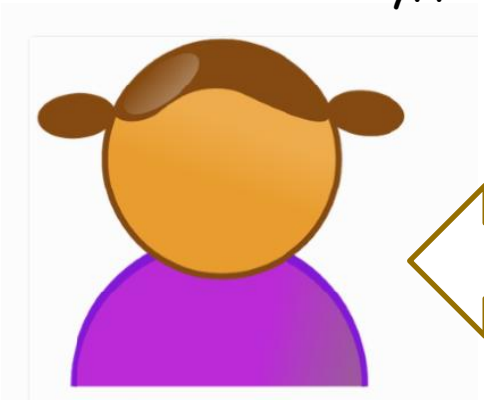
Задание для самостоятельной работы

- Составьте свой численный пример (четыре итерации) работы протокола Фиата-Шамира, три итерации, когда оба участника действуют честно; одна, когда один из участников протокола - злоумышленник
- Проанализировать вопрос правильного выбора параметров p и q

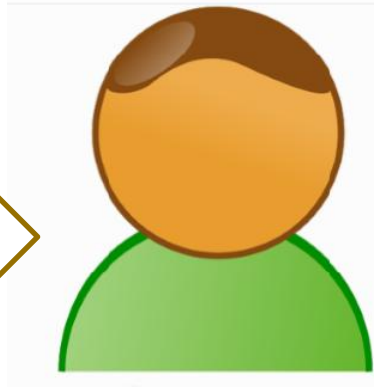
Протокол Фейга-Фиата-Шамира



Протокол асимметричной аутентификации удаленных абонентов Диффи-Хеллмана



Ненадежный канал связи



Алиса

Боб

Выработка общего секретного ключа K_{AB}

Электронная подпись

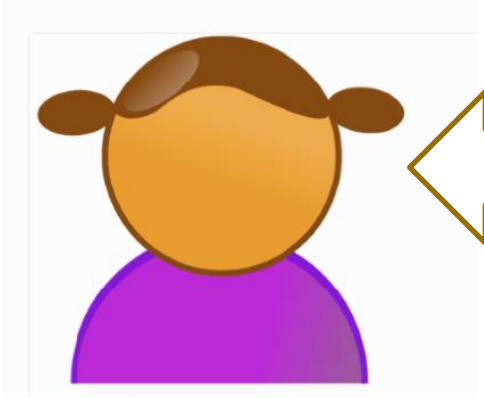
Электронная подпись

Симметричное шифрование

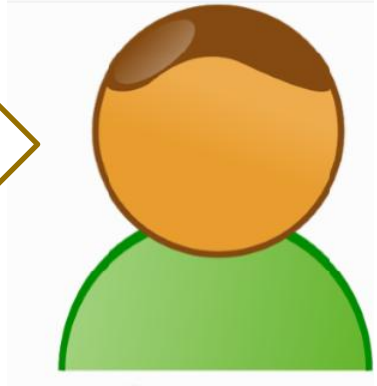
Симметричное шифрование

Проверка электронной подписи

Проверка электронной подписи



Ненадежный канал связи



Алиса

Боб

A: 1) x_A; 2) $y_A = \omega^{x_A} \bmod p \rightarrow B$

B: 1) x_B; 2) $y_B = \omega^{x_B} \bmod p$; 3) $SK_B\{y_A, y_B\}$; 4) $K_{AB} = \omega^{x_A x_B} \bmod p$;
5) $z_B = K_{AB}\{SK_B\{y_A, y_B\}\}$; 6) $(y_B, z_B) \rightarrow A$

A: 1) $K_{AB} = \omega^{x_A x_B} \bmod p$; 2) $SK_A\{y_A, y_B\}$;
3) $z_A = K_{AB}\{SK_A\{y_A, y_B\}\} \rightarrow B$

A: 1) $K_{AB}\{z_B\}$; 2) $PK_B\{K_{AB}\{z_B\}\} = \{y_A, y_B\}$?

B: 1) $K_{AB}\{z_A\}$; 2) $PK_A\{K_{AB}\{z_A\}\} = \{y_A, y_B\}$?

- ✓ Классическая электронная подпись → ✓ Вероятностная электронная подпись
- ✓ Протокол подписания контракта
- ✓ Групповая электронная подпись
- ✓ Неотвергаемая электронная подпись

ЭПС – самый сложный объект с точки зрения решения задачи ОБИ

Определить потенциальный источник угрозы практически невозможно

Для каждого участника надо предполагать, что остальные участники процесса объединились, чтобы его обмануть

- ✓ Слепая электронная подпись → Цифровые деньги
- ✓ Одноразовая кольцевая подпись → Виртуальные деньги
- ✓ Двойная электронная подпись → Электронные деньги

...

The questions are welcome !