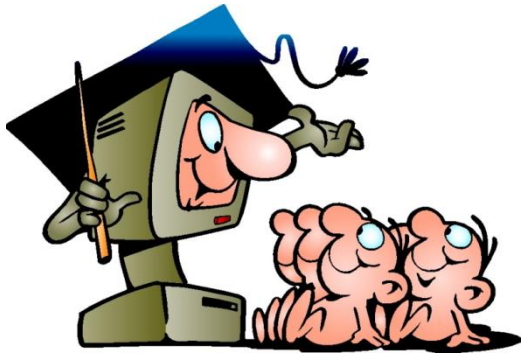
КС&Т Кафедра 12 НИЯУ МИФИ

Защита информации

Иванов М.А.

Криптосистемы с открытым ключом



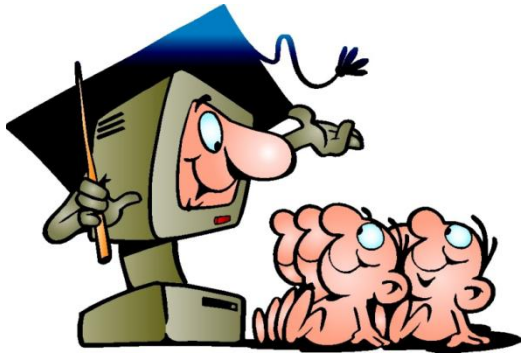
Москва, 2025

КС&Т Кафедра 12 НИЯУ МИФИ

Защита информации

Иванов М.А.

Криптосистемы с открытым ключом

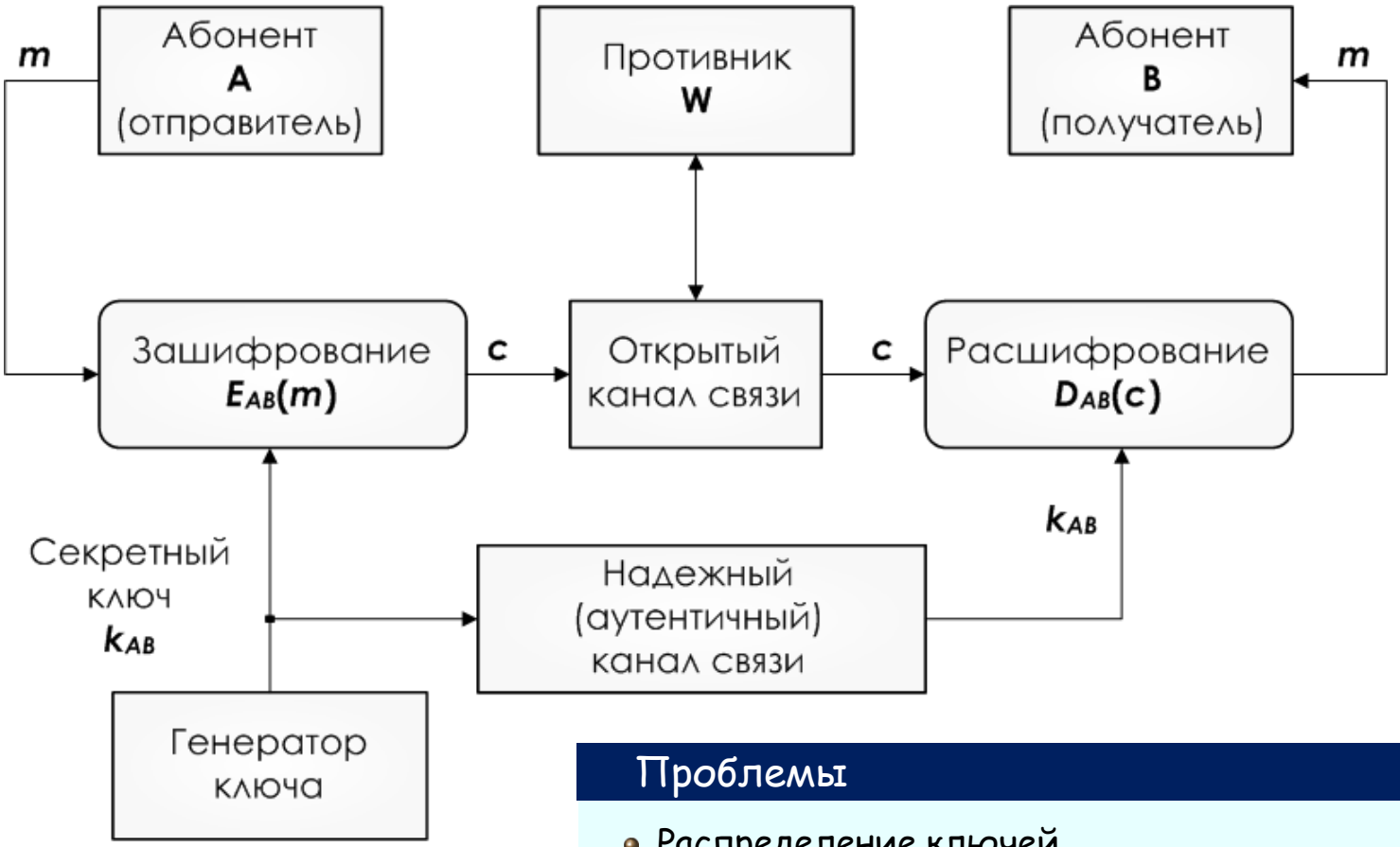


Москва, 2025

Темы

- Модель криптосистемы с открытым ключом
- Односторонняя функция, односторонняя функция с секретом
- Криптосистема RSA
- Идея электронной подписи
- Протокол выработки общего секретного ключа

Криптосистема с секретным ключом

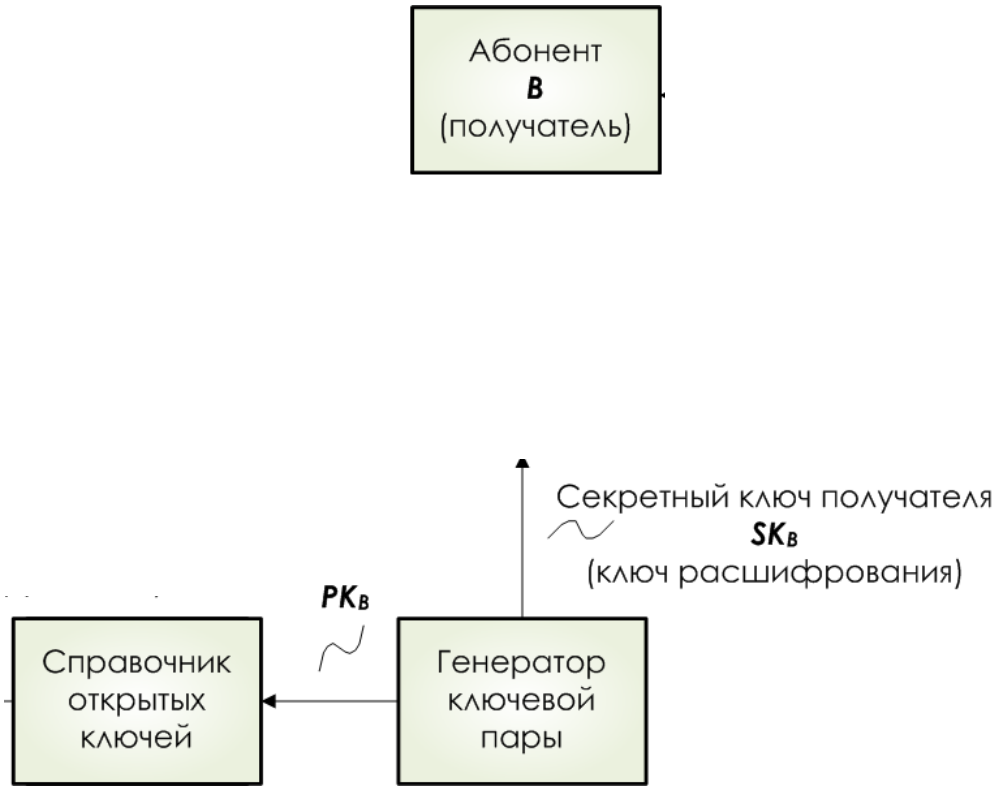


Проблемы

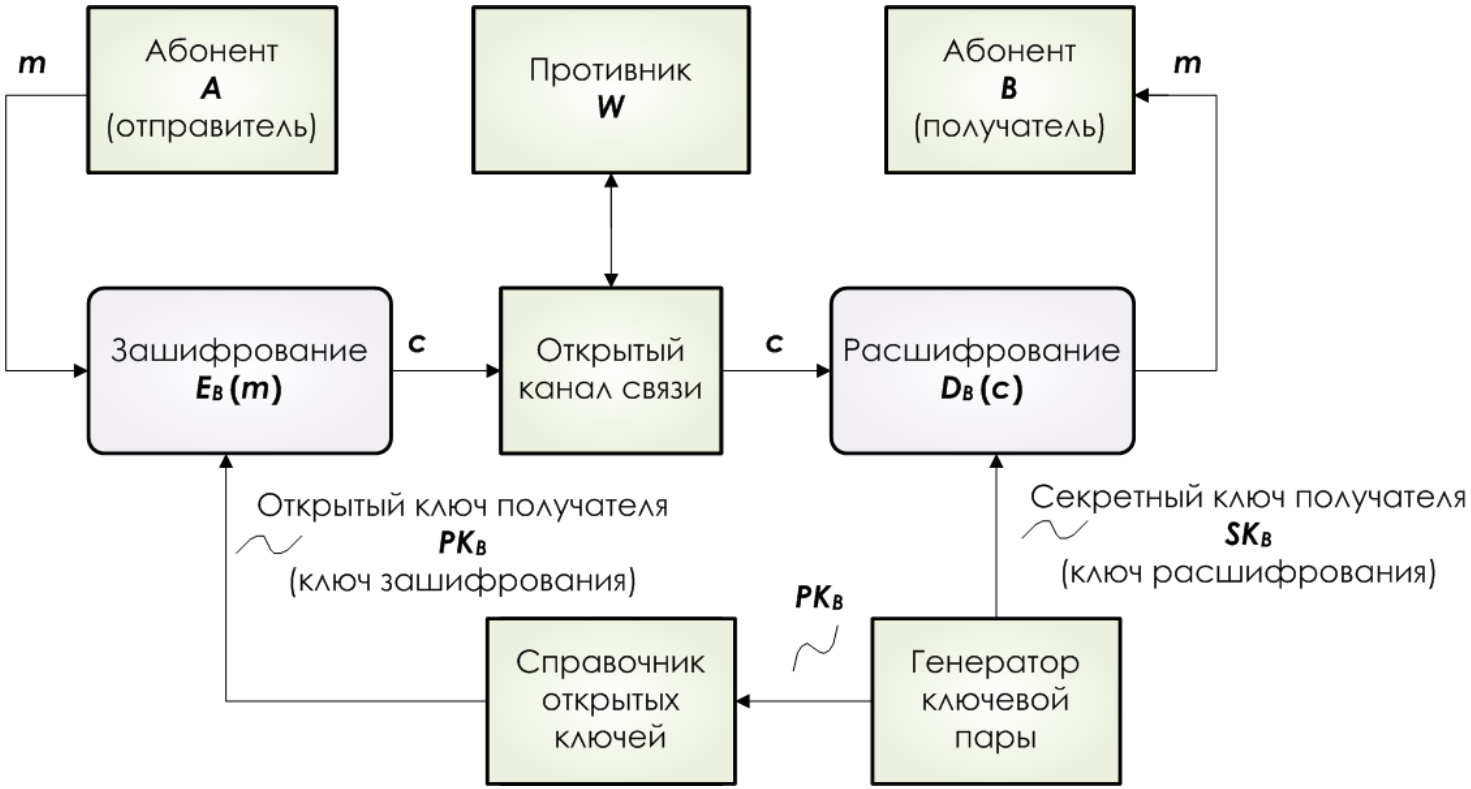
- Распределение ключей
- Отсутствие юридической значимости пересылаемых электронных документов

Криптосистема с открытым ключом

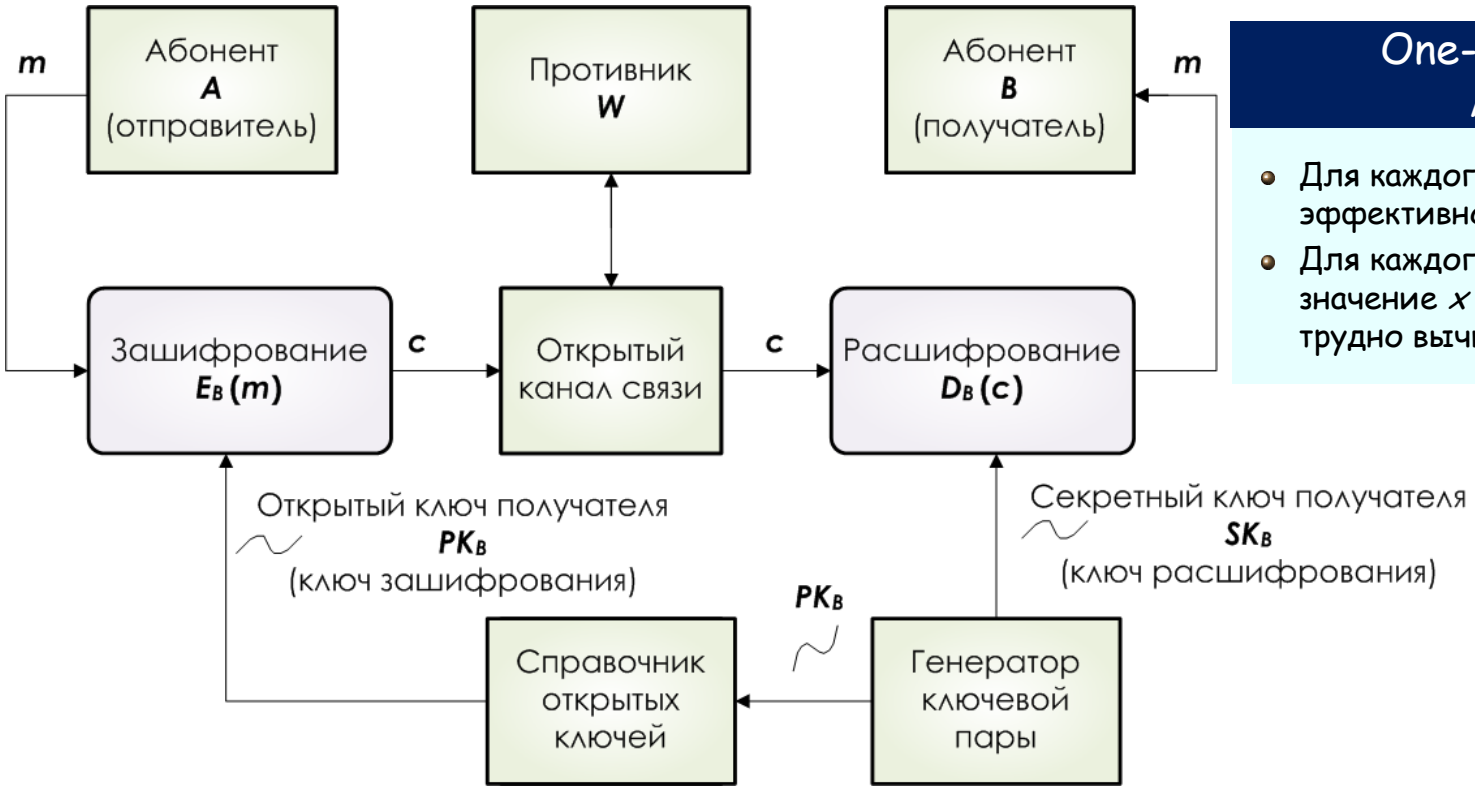
Криптосистема с открытым ключом



Криптосистема с открытым ключом



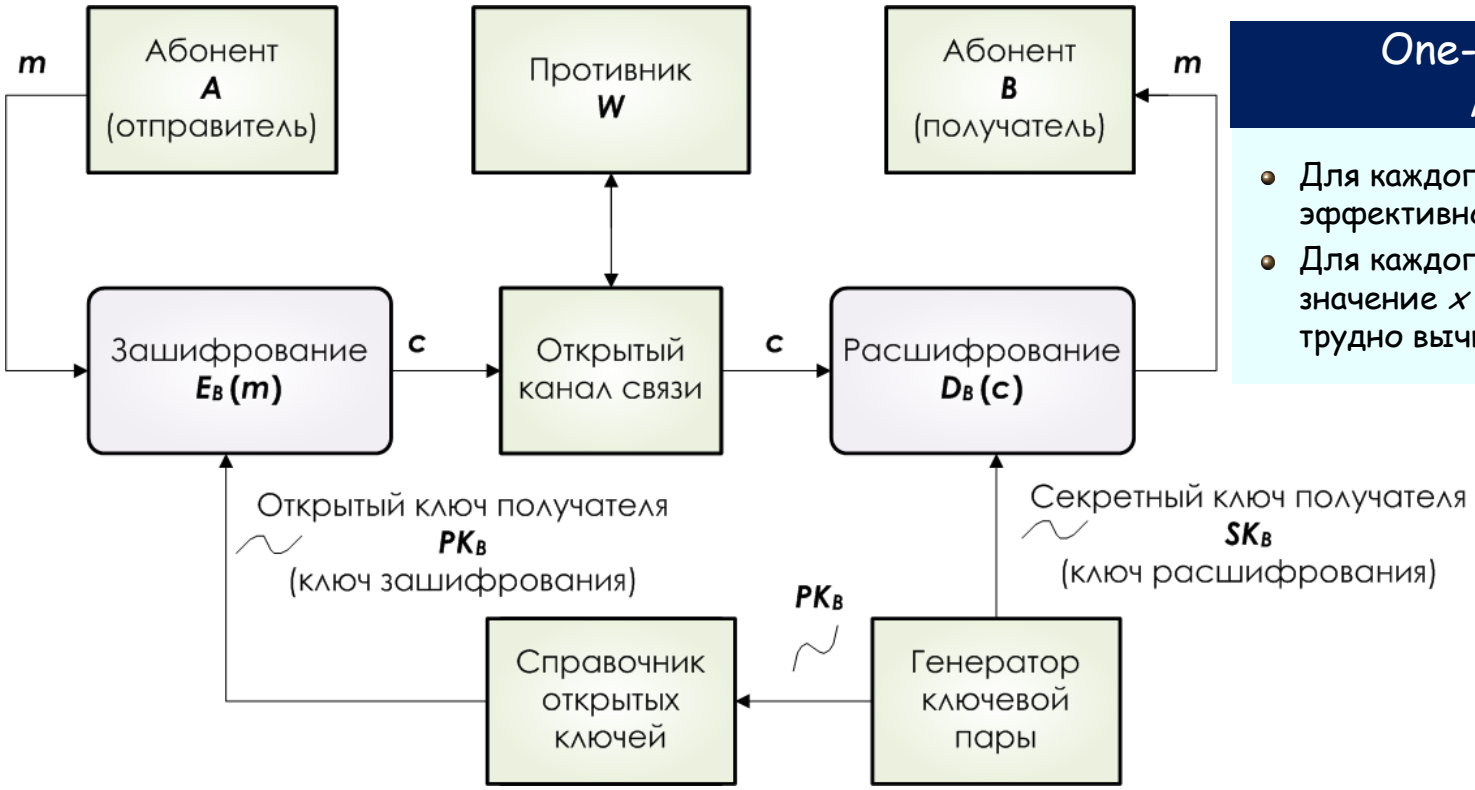
Криптосистема с открытым ключом



One-way Function
$F: X \rightarrow Y$

- Для каждого $x \in X$, значение $F(x)$ эффективно вычисляется
- Для каждого $y \in F[X]$, значение $x \in X$, такое, что $F(x) = y$, трудно вычислимо

Криптосистема с открытым ключом

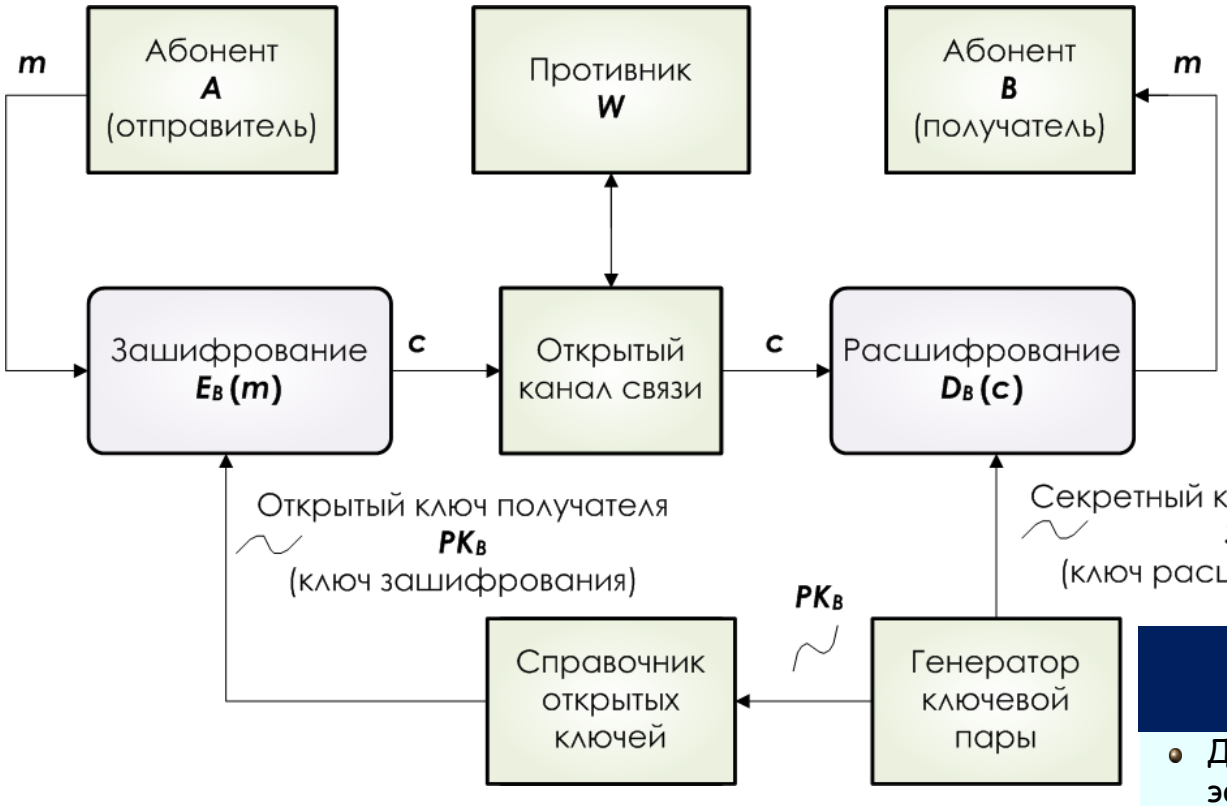


One-way Function
$F: X \to Y$

- Для каждого $x \in X$, значение $F(x)$ эффективно вычисляется
- Для каждого $y \in F[X]$, значение $x \in X$, такое, что $F(x) = y$, трудно вычислимо

$$y = g^x \bmod p$$
$$y = x^2 \bmod p$$

Криптосистема с открытым ключом



One-way Function
$F: X \to Y$

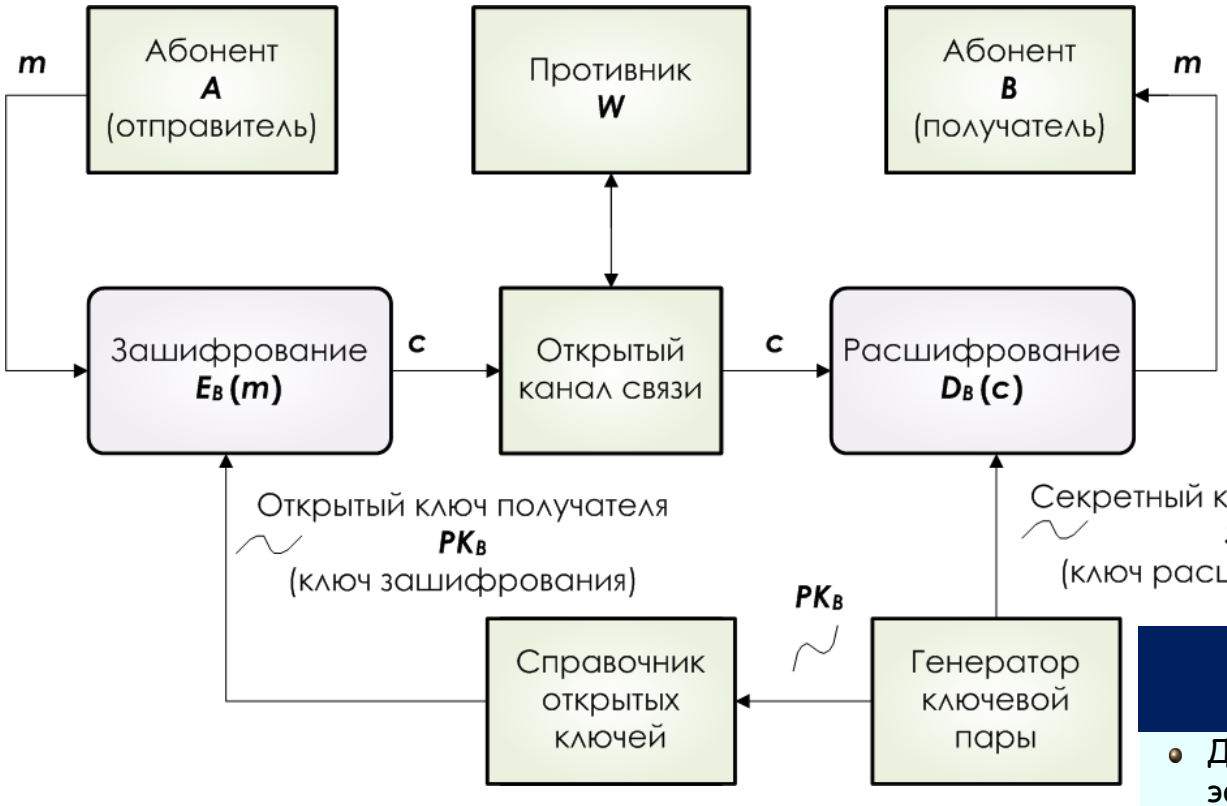
- Для каждого $x \in X$, значение $F(x)$ эффективно вычисляется
- Для каждого $y \in F[X]$, значение $x \in X$, такое, что $F(x) = y$, трудно вычислимо

$$y = g^x \bmod p$$
$$y = x^2 \bmod p$$

One-way Trapdoor Function
$F_k: X \to Y$

- Для каждого $x \in X$, значение $F_k(x)$ эффективно вычисляется
- Если k неизвестно, для каждого $y \in F_k[X]$, значение $x \in X$, такое, что $F_k(x) = y$, трудно вычислимо
- Если k известно, для каждого $y \in F_k[X]$, значение $x \in X$, такое, что $F_k(x) = y$, эффективно вычисляется

Криптосистема с открытым ключом



One-way Function
$F: X \to Y$

- Для каждого $x \in X$, значение $F(x)$ эффективно вычисляется
- Для каждого $y \in F[X]$, значение $x \in X$, такое, что $F(x) = y$, трудно вычислимо

$$y = g^x \bmod p$$
$$y = x^2 \bmod p$$

One-way Trapdoor Function
$F_k: X \to Y$

- Для каждого $x \in X$, значение $F_k(x)$ эффективно вычисляется
- Если k неизвестно, для каждого $y \in F_k[X]$, значение $x \in X$, такое, что $F_k(x) = y$, трудно вычислимо
- Если k известно, для каждого $y \in F_k[X]$, значение $x \in X$, такое, что $F_k(x) = y$, эффективно вычисляется

Проблемы

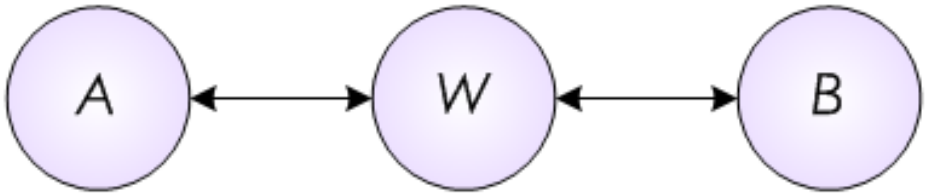
- Низкое быстродействие
- Возможность подмены открытых ключей

Атака Man-in-the-middle

COK

A	pk_A
B	pk_B

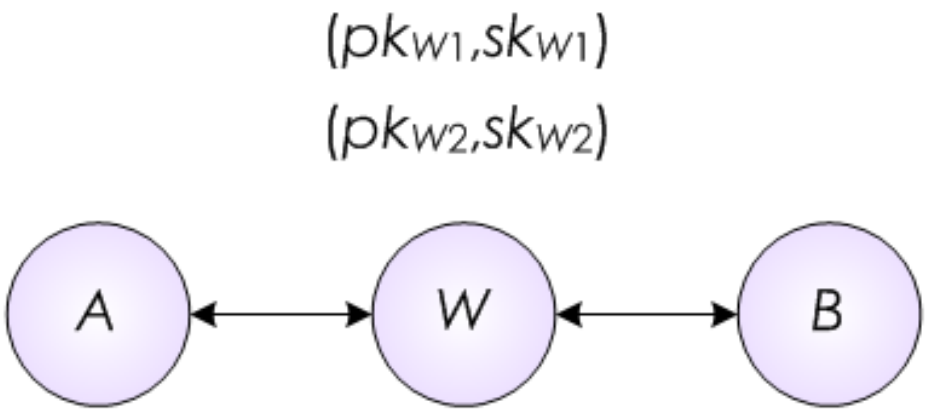
Атака Man-in-the-middle



COK

A	pk_A
B	pk_B

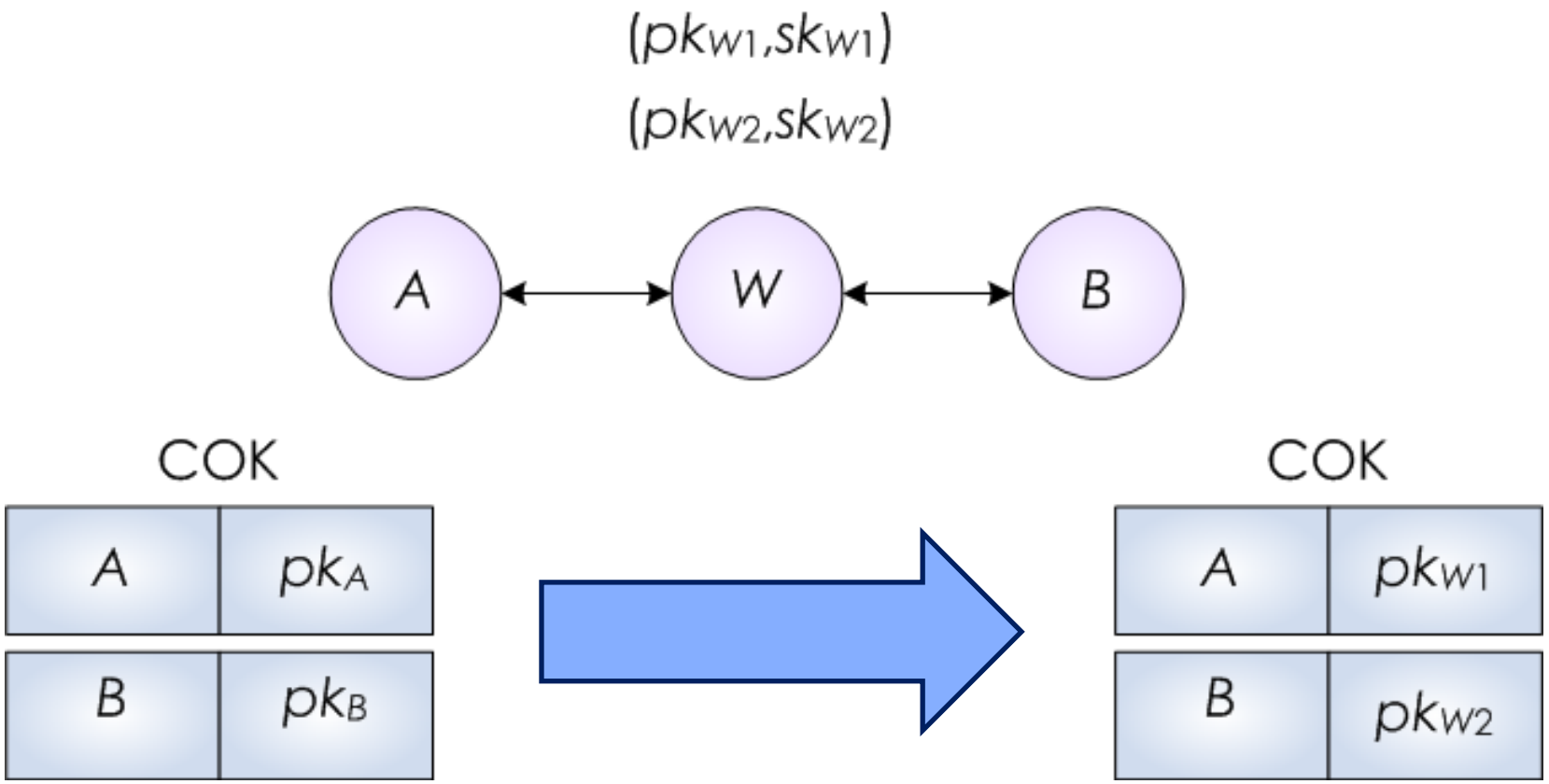
Атака Man-in-the-middle



COK

A	pk_A
B	pk_B

Атака Man-in-the-Middle



Криптосистема RSA (Rivest, Shamir, Adleman)

Построение криптосистемы

Пример

Криптосистема RSA

Построение криптосистемы

- Выбираем два различных простых числа p и q

Пример

- $p = 3$, $q = 11$

Криптосистема RSA

Построение криптосистемы

- Выбираем два различных простых числа p и q
- Вычисляем $N = pq$

Пример

- $p = 3$, $q = 11$
- $N = 3 \cdot 11 = 33$

Криптосистема RSA

Построение криптосистемы

- Выбираем два различных простых числа p и q
- Вычисляем $N = pq$
- Вычисляем $\varphi(N) = (p - 1)(q - 1)$

Пример

- $p = 3$, $q = 11$
- $N = 3 \cdot 11 = 33$
- $\varphi(N) = 2 \cdot 10 = 20$

Криптосистема RSA

Построение криптосистемы

- Выбираем два различных простых числа p и q
- Вычисляем $N = pq$
- Вычисляем $\varphi(N) = (p - 1)(q - 1)$
- Находим такое e, что $\gcd(e, \varphi(N)) = 1$

Пример

- $p = 3$, $q = 11$
- $N = 3 \cdot 11 = 33$
- $\varphi(N) = 2 \cdot 10 = 20$
- $\gcd(7, 20) = 1 \rightarrow e = 7$

Криптосистема RSA

Построение криптосистемы

- Выбираем два различных простых числа p и q
- Вычисляем $N = pq$
- Вычисляем $\varphi(N) = (p - 1)(q - 1)$
- Находим такое e, что $\gcd(e, \varphi(N)) = 1$
- Находим такое d, что $ed \equiv 1 \bmod \varphi(N)$

Пример

- $p = 3$, $q = 11$
- $N = 3 \cdot 11 = 33$
- $\varphi(N) = 2 \cdot 10 = 20$
- $\gcd(7, 20) = 1 \rightarrow e = 7$
- $3 \cdot 7 \equiv 1 \bmod 20 \rightarrow d = 3$

Криптосистема RSA

Построение криптосистемы

- Выбираем два различных простых числа p и q
- Вычисляем $N = pq$
- Вычисляем $\varphi(N) = (p - 1)(q - 1)$
- Находим такое e, что $\gcd(e, \varphi(N)) = 1$
- Находим такое d, что $ed \equiv 1 \bmod \varphi(N)$

Для любого x справедливо

$x^{ed} \bmod N = x$

Пример

- $p = 3$, $q = 11$
- $N = 3 \cdot 11 = 33$
- $\varphi(N) = 2 \cdot 10 = 20$
- $\gcd(7, 20) = 1 \rightarrow e = 7$
- $3 \cdot 7 \equiv 1 \bmod 20 \rightarrow d = 3$

Криптосистема RSA

Построение криптосистемы

- Выбираем два различных простых числа p и q
- Вычисляем $N = pq$
- Вычисляем $\varphi(N) = (p - 1)(q - 1)$
- Находим такое e, что $\gcd(e, \varphi(N)) = 1$
- Находим такое d, что $ed \equiv 1 \bmod \varphi(N)$

⇩

Для любого x справедливо

$x^{ed} \bmod N = x$

⇩

(e, N) – Public Key, d – Secret Key

$c = m^e \bmod N$ - Encryption

$m = c^d \bmod N$ - Decryption

Пример

- $p = 3$, $q = 11$
- $N = 3 \cdot 11 = 33$
- $\varphi(N) = 2 \cdot 10 = 20$
- $\gcd(7, 20) = 1 \rightarrow e = 7$
- $3 \cdot 7 \equiv 1 \bmod 20 \rightarrow d = 3$

Криптосистема RSA

Построение криптосистемы

- Выбираем два различных простых числа p и q
- Вычисляем $N = pq$
- Вычисляем $\varphi(N) = (p - 1)(q - 1)$
- Находим такое e, что $\gcd(e, \varphi(N)) = 1$
- Находим такое d, что $ed \equiv 1 \bmod \varphi(N)$

⇩

Для любого x справедливо

$x^{ed} \bmod N = x$

⇩

(e, N) – Public Key, d – Secret Key

$c = m^e \bmod N$ - Encryption

$m = c^d \bmod N$ - Decryption

Пример

- $p = 3$, $q = 11$
- $N = 3 \cdot 11 = 33$
- $\varphi(N) = 2 \cdot 10 = 20$
- $\gcd(7, 20) = 1 \rightarrow e = 7$
- $3 \cdot 7 \equiv 1 \bmod 20 \rightarrow d = 3$

⇩

(7, 33) – Public Key, 3 – Secret Key

$m = 2$

$c = 2^7 \bmod 33 = 29$ - Encryption

$m = 29^3 \bmod 33 = 2$ - Decryption

Криптосистема RSA

Построение криптосистемы

- Выбираем два различных простых числа p и q
- Вычисляем $N = pq$
- Вычисляем $\varphi(N) = (p - 1)(q - 1)$
- Находим такое e, что $\gcd(e, \varphi(N)) = 1$
- Находим такое d, что $ed \equiv 1 \bmod \varphi(N)$

⇩

Для любого x справедливо

$x^{ed} \bmod N = x$

⇩

(e, N) – Public Key, d – Secret Key

$c = m^e \bmod N$ - Encryption

$m = c^d \bmod N$ - Decryption

Пример

- $p = 3$, $q = 11$
- $N = 3 \cdot 11 = 33$
- $\varphi(N) = 2 \cdot 10 = 20$
- $\gcd(7, 20) = 1 \rightarrow e = 7$
- $3 \cdot 7 \equiv 1 \bmod 20 \rightarrow d = 3$

⇩

(7, 33) – Public Key, 3 – Secret Key

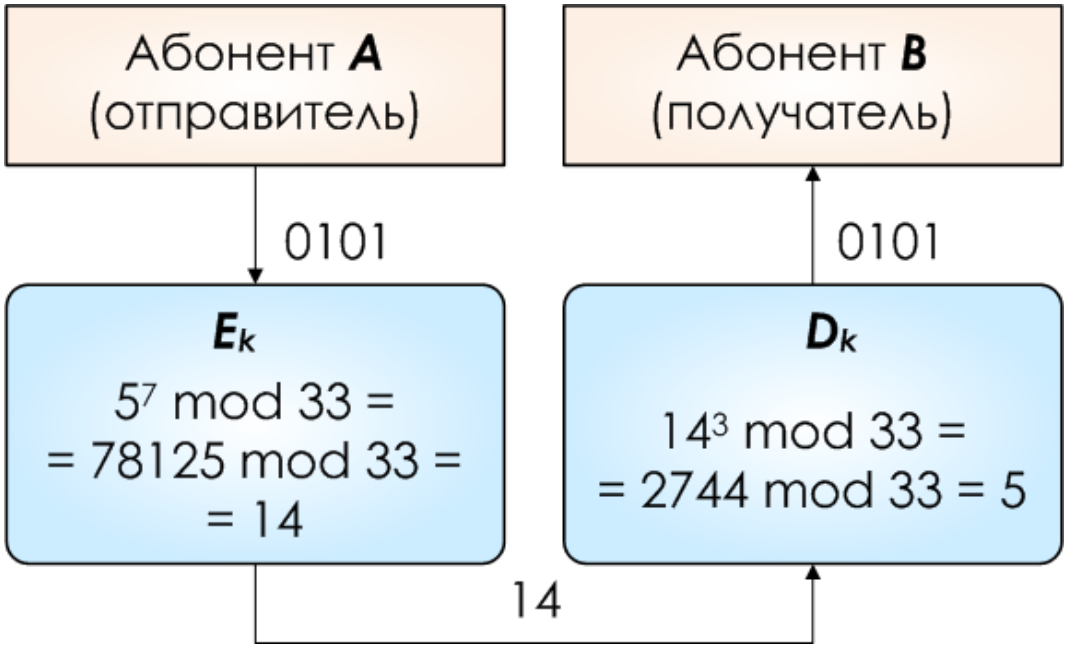
$m = 2$

$c = 2^7 \bmod 33 = 29$ - Encryption

$m = 29^3 \bmod 33 = 2$ - Decryption

Стойкость криптосистемы RSA основана на сложности решения задачи факторизации целых чисел

Пример шифрования по схеме RSA



Пример шифрования по схеме RSA

Пример авторов RSA

Пример шифрования по схеме RSA

Пример авторов RSA

Открытый текст ITS ALL GREEK TO ME

Пример шифрования по схеме RSA

Пример авторов RSA

Открытый текст ITS ALL GREEK TO ME

Кодирование: пробел – 00, буква A – 01, буква B – 02, ... , буква Z – 26

Пример шифрования по схеме RSA

Пример авторов RSA

Открытый текст ITS ALL GREEK TO ME

Кодирование: пробел – 00, буква A – 01, буква B – 02, ... , буква Z – 26

m = 09201900011212000718050511002015001305

Пример шифрования по схеме RSA

Пример авторов RSA

Открытый текст ITS ALL GREEK TO ME[1]

Кодирование[1]: пробел – 00, буква A – 01, буква B – 02, ... , буква Z – 26

m = 09201900011212000718050511002015001305[1]

e = 9007, N =
114381625757888867669235779976146612010218296721242362562651842935706952457338978305971235639587050589890751475992900268795435 41

$|p| = 64_{10}$[1], $|q| = 65_{10}$[1]

[1] Эта информация не публиковалась

Пример шифрования по схеме RSA

Пример авторов RSA

Открытый текст ITS ALL GREEK TO ME[1]

Кодирование[1]: пробел – 00, буква A – 01, буква B – 02, ... , буква Z – 26

m = 09201900011212000718050511002015001305[1]

e = 9007, N =
114381625757888867669235779976146612010218296721242362562651842935706952457338978305971235639587050589890751475992900268795435 41

$|p|$ = 64_{10}[1], $|q|$ = 65_{10} [1]

c =
199935131497805100452317122740260647423204017058391463103703717406259716089489275043992096267258267501289355446135382376974802 6

[1] Эта информация не публиковалась

Временная атака на RSA

(e, N) – Public Key, d – Secret Key

$c = m^e \bmod N$ - Encryption

$m = c^d \bmod N$ - Decryption

Временная атака на RSA

(e, N) – Public Key, d – Secret Key

$c = m^e \bmod N$ - Encryption

$m = c^d \bmod N$ - Decryption

Если время выполнения операций E и D зависит от исходных данных, возможна атака на данную конкретную реализацию

Временная атака на RSA

(e, N) – Public Key, d – Secret Key

$c = m^e \bmod N$ - Encryption

$m = c^d \bmod N$ - Decryption

Если время выполнения операций E и D зависит от исходных данных, возможна атака на данную конкретную реализацию

При реализации криптографических алгоритмов ЗИ нужно учитывать возможность атак, основанных на утечке информации по побочным каналам (Side Channel Attacks)

Протокол выработки общего секретного ключа

$y = g^x \bmod p$ – односторонняя функция

p – простое число,

g - примитивный элемент поля $GF(p)$

Протокол выработки общего секретного ключа

$y = g^x \bmod p$ – односторонняя функция

p – простое число,

g - примитивный элемент поля $GF(p)$

Протокол Диффи-Хеллмана

Протокол выработки общего секретного ключа

$y = g^x \bmod p$ – односторонняя функция

p – простое число,

g - примитивный элемент поля $GF(p)$

Протокол Диффи-Хеллмана

- Абоненты A и B независимо друг от друга вырабатывают два случайных числа соответственно x_A и x_B, которые держат в секрете

Протокол выработки общего секретного ключа

$y = g^x \bmod p$ – односторонняя функция

p – простое число,

g - примитивный элемент поля $GF(p)$

Протокол Диффи-Хеллмана

- Абоненты A и B независимо друг от друга вырабатывают два случайных числа соответственно x_A и x_B, которые держат в секрете
- Абоненты A и B вычисляют значения $y_A = g^{x_A} \bmod p$ и $y_B = g^{x_B} \bmod p$

Протокол выработки общего секретного ключа

$y = g^x \bmod p$ – односторонняя функция

p – простое число,

g - примитивный элемент поля $GF(p)$

Протокол Диффи-Хеллмана

- Абоненты A и B независимо друг от друга вырабатывают два случайных числа соответственно x_A и x_B, которые держат в секрете
- Абоненты A и B вычисляют значения $y_A = g^{x_A} \bmod p$ и $y_B = g^{x_B} \bmod p$
- Абоненты A и B обмениваются сообщениями y_A и y_B

Протокол выработки общего секретного ключа

$y = g^x \bmod p$ – односторонняя функция

p – простое число,

g - примитивный элемент поля $GF(p)$

Протокол Диффи-Хеллмана

- Абоненты A и B независимо друг от друга вырабатывают два случайных числа соответственно x_A и x_B, которые держат в секрете
- Абоненты A и B вычисляют значения $y_A = g^{x_A} \bmod p$ и $y_B = g^{x_B} \bmod p$
- Абоненты A и B обмениваются сообщениями y_A и y_B
- A, получив сообщение y_B, вычисляет значение $(y_B)^{x_A} \bmod p = (g^{x_B})^{x_A} \bmod p$;
  B, получив сообщение y_A, вычисляет значение $(y_A)^{x_B} \bmod p = (g^{x_A})^{x_B} \bmod p$

Протокол выработки общего секретного ключа

$y = g^x \bmod p$ – односторонняя функция

p – простое число,

g - примитивный элемент поля $GF(p)$

Протокол Диффи-Хеллмана

- Абоненты A и B независимо друг от друга вырабатывают два случайных числа соответственно x_A и x_B, которые держат в секрете
- Абоненты A и B вычисляют значения $y_A = g^{x_A} \bmod p$ и $y_B = g^{x_B} \bmod p$
- Абоненты A и B обмениваются сообщениями y_A и y_B
- A, получив сообщение y_B, вычисляет значение $(y_B)^{x_A} \bmod p = (g^{x_B})^{x_A} \bmod p$; B, получив сообщение y_A, вычисляет значение $(y_A)^{x_B} \bmod p = (g^{x_A})^{x_B} \bmod p$
- Число, равное $g^{x_A x_B} \bmod p$, объявляется общим секретным ключом K_{AB}

На чем основана стойкость протокола Диффи-Хеллмана?

Что в нем не так?

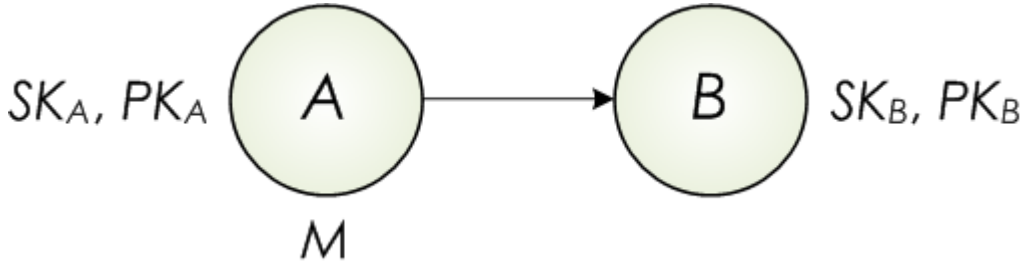
1) Нужна предварительная взаимная аутентификация абонентов A и B

2) Key Derivation Function

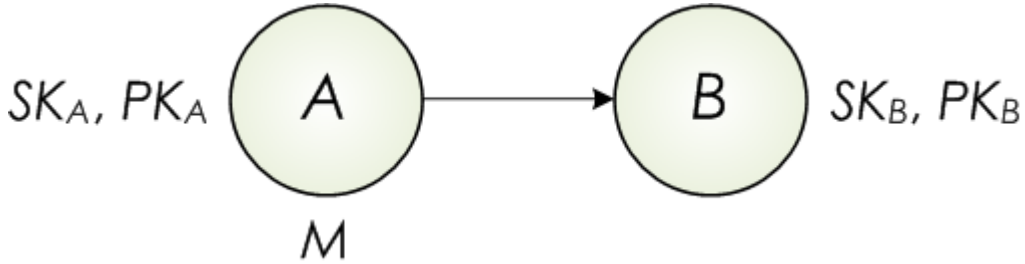
3) Число p должно быть «хорошим» простым числом

Идея электронной подписи (ЭП)

Идея электронной подписи (ЭП)



Идея электронной подписи (ЭП)



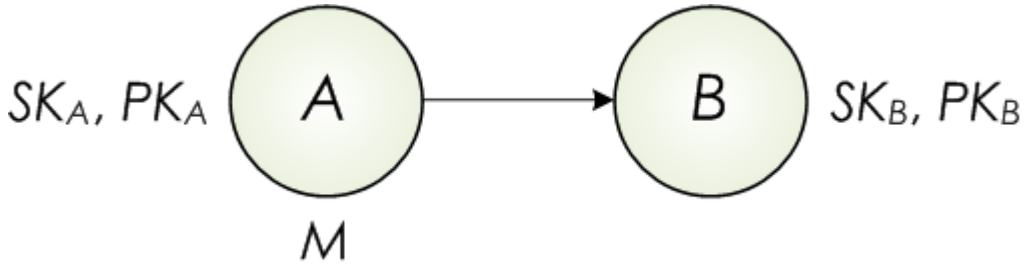
Вариант № 1

- Абонент *A* формирует сообщение $y_A = PK_B\{SK_A\{M\}\}$ и отправляет его абоненту *B*
- Абонент *B* читает документ $M = PK_A\{SK_B\{y_A\}\}$

$$y'_A = SK_A\{M\} \rightarrow y_A = PK_B\{y'_A\}$$

$$M' = SK_B\{y_A\} \rightarrow M = PK_A\{M'\}$$

Идея электронной подписи (ЭП)



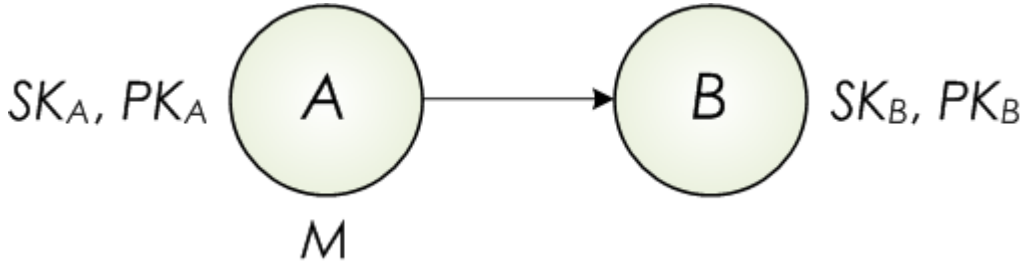
Вариант № 1

- Абонент *A* формирует сообщение $y_A = PK_B\{SK_A\{M\}\}$ и отправляет его абоненту *B*
- Абонент *B* читает документ $M = PK_A\{SK_B\{y_A\}\}$

Вариант № 2

- Абонент *A* формирует сообщение $y_A = SK_A\{PK_B\{M\}\}$ и отправляет его абоненту *B*
- Абонент *B* читает документ $M = SK_B\{PK_A\{y_A\}\}$

Идея электронной подписи (ЭП)



Вариант № 1

- Абонент *A* формирует сообщение $y_A = PK_B\{SK_A\{M\}\}$ и отправляет его абоненту *B*
- Абонент *B* читает документ $M = PK_A\{SK_B\{y_A\}\}$

Вариант № 2

- Абонент *A* формирует сообщение $y_A = SK_A\{PK_B\{M\}\}$ и отправляет его абоненту *B*
- Абонент *B* читает документ $M = SK_B\{PK_A\{y_A\}\}$

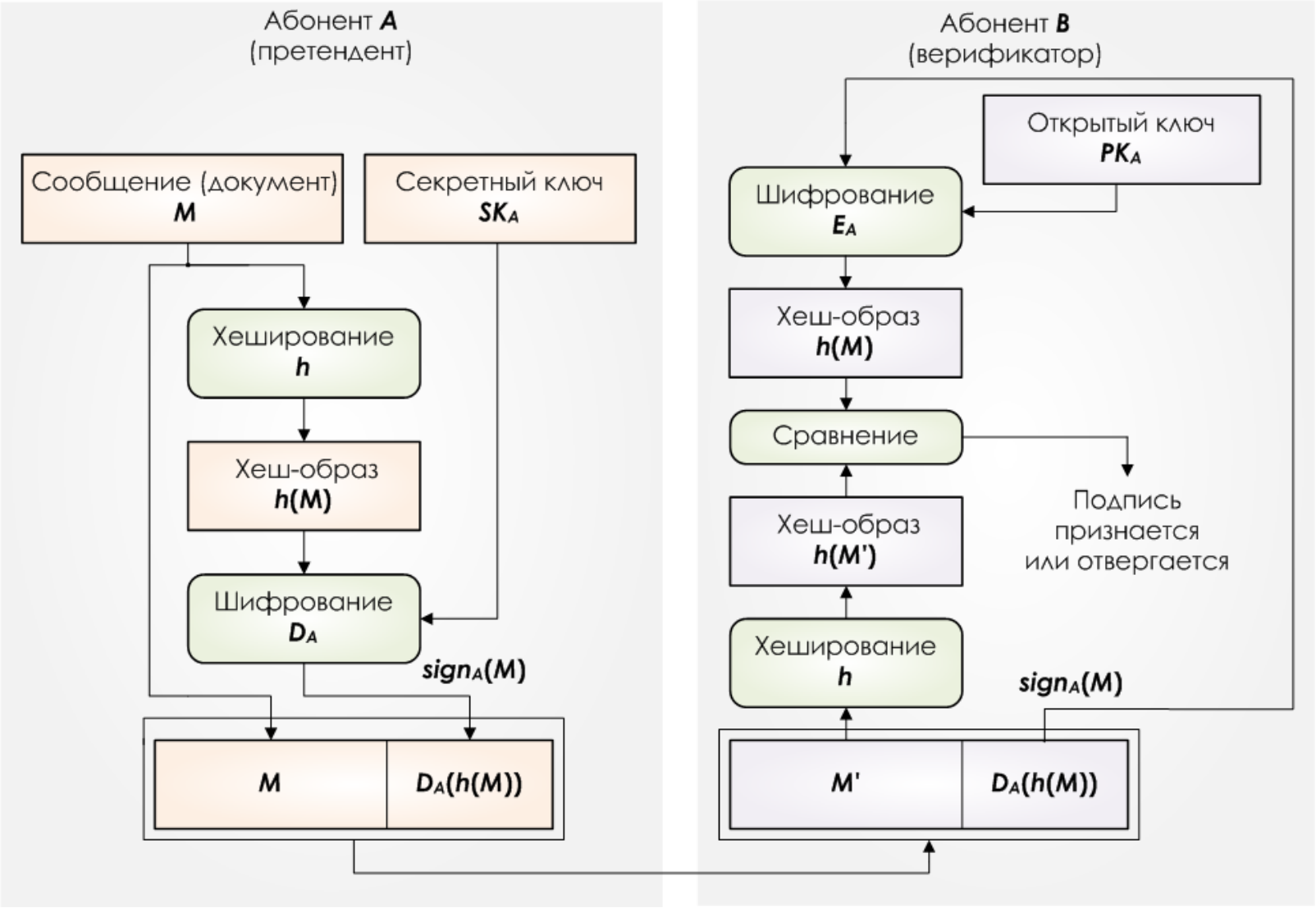
Почему?

Что во втором случае не так?

Формирование ЭП – шифрование документа на секретном ключе отправителя

Проверка ЭП – шифрование ЭП на открытом ключе отправителя …

Протокол классической ЭП



Формирование классической ЭП – шифрование хеша документа на секретном ключе отправителя

Проверка классической ЭП – шифрование ЭП на открытом ключе отправителя …

The questions are welcome !