Схема цифровой подписи

Схема цифровой подписи RSA

Тазаева Анастасия Анатольевна

2025-11-11

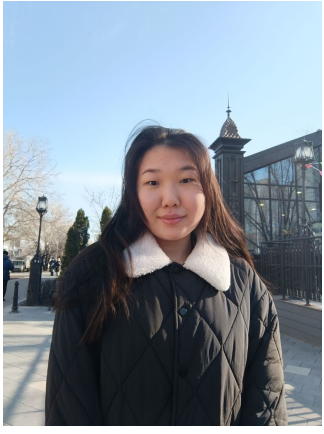
Содержание I

Раздел 1

1. Информация

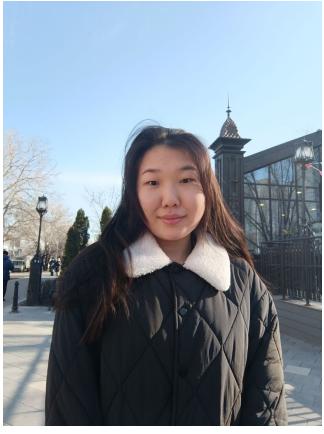
1.1 Докладчик

- Тазаева Анастасия Анатольевна



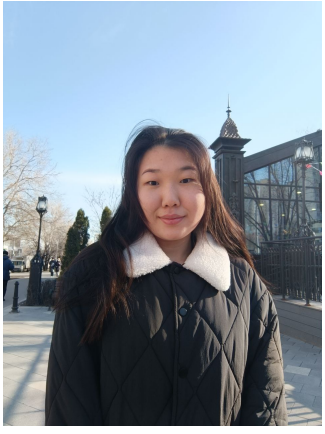
1.1 Докладчик

- Тазаева Анастасия Анатольевна
- студент группы НФИмд-02-25



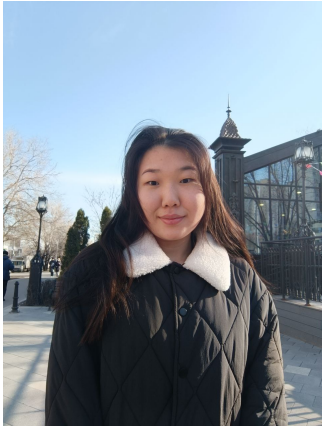
1.1 Докладчик

- Тазаева Анастасия Анатольевна
- студент группы НФИмд-02-25
- Российский университет дружбы народов им. П. Лумумбы



1.1 Докладчик

- Тазаева Анастасия Анатольевна
- студент группы НФИмд-02-25
- Российский университет дружбы народов им. П. Лумумбы
- 1032259385@pfur.ru



Раздел 2

2. Вводная часть

2.1 Актуальность

- RSA - один из первых криптографических алгоритмов, предложенный в 1977 году.

2.1 Актуальность

- RSA - один из первых криптографических алгоритмов, предложенный в 1977 году.
- Цифровая подпись RSA имеет широкое практическое применение (защищенные веб-соединения, инфраструктура открытых ключей, электронный документооборот и юридически значимые подписи, подписание ПО и обновлений)

2.1 Актуальность

- RSA - один из первых криптографических алгоритмов, предложенный в 1977 году.
- Цифровая подпись RSA имеет широкое практическое применение (защищенные веб-соединения, инфраструктура открытых ключей, электронный документооборот и юридически значимые подписи, подписание ПО и обновлений)
- RSA служит классическим примером для изучения асимметричного шифрования, математических основ криптографии (факторизация больших чисел) и принципов работы цифровых подписей.

2.2 Объект и предмет исследования

- Алгоритм подписи и проверки цифровой подписи RSA

2.3 Цели и задачи

Сформировать целостное представление о схеме цифровой подписи RSA:

- Описать алгоритм цифровой подписи;

2.3 Цели и задачи

Сформировать целостное представление о схеме цифровой подписи RSA:

- Описать алгоритм цифровой подписи;
- Выявить уязвимости и методы защиты.

2.4 Что такое схема цифровой подписи RSA?

Схема цифровой подписи RSA - механизм, основанный на асимметричном алгоритме RSA (Rivest-Shamir-Adleman). Он позволяет создавать электронную цифровую подпись (ЭЦП), которая подтверждает подлинности и целостность сообщения.

2.5 Алгоритм схемы цифровой подписи RSA

1. Генерация ключей (e, d, n).

2.5 Алгоритм схемы цифровой подписи RSA

1. Генерация ключей (e, d, n).
2. Хэш сообщения: $H(m)$.

2.5 Алгоритм схемы цифровой подписи RSA

1. Генерация ключей (e, d, n).
2. Хэш сообщения: $H(m)$.
3. Подпись: $H(m)^d mod n$

2.5 Алгоритм схемы цифровой подписи RSA

1. Генерация ключей (e, d, n).
2. Хэш сообщения: $H(m)$.
3. Подпись: $H(m)^d mod n$
4. Передача (m,подпись).

2.5 Алгоритм схемы цифровой подписи RSA

1. Генерация ключей (e, d, n).
2. Хэш сообщения: $H(m)$.
3. Подпись: $H(m)^d mod n$
4. Передача (m,подпись).
5. Проверка.

2.6 Алгоритм схемы цифровой подписи RSA. Генерация ключей и хэш сообщения

1. Генерация ключей

2.6 Алгоритм схемы цифровой подписи RSA. Генерация ключей и хэш сообщения

1. Генерация ключей

- Выбираются большие простые числа p и q.

2.6 Алгоритм схемы цифровой подписи RSA. Генерация ключей и хэш сообщения

1. Генерация ключей

- Выбираются большие простые числа p и q.
- Вычисляется модуль $n = p \cdot q$ и функция Эйлера $\Psi(n)$.

2.6 Алгоритм схемы цифровой подписи RSA. Генерация ключей и хэш сообщения

1. Генерация ключей

- Выбираются большие простые числа p и q.
- Вычисляется модуль $n = p \cdot q$ и функция Эйлера $\Psi(n)$.
- Выбирается открытый ключ e (взаимно простой с $\Psi(n)$).

2.6 Алгоритм схемы цифровой подписи RSA. Генерация ключей и хэш сообщения

1. Генерация ключей

- Выбираются большие простые числа p и q.
- Вычисляется модуль $n = p \cdot q$ и функция Эйлера $\Psi(n)$.
- Выбирается открытый ключ e (взаимно простой с $\Psi(n)$).
- Находится закрытый ключ d: $d = e^{-1}(mod\Psi(n)$.

2.6 Алгоритм схемы цифровой подписи RSA. Генерация ключей и хэш сообщения

1. Генерация ключей

- Выбираются большие простые числа p и q.
- Вычисляется модуль $n = p \cdot q$ и функция Эйлера $\Psi(n)$.
- Выбирается открытый ключ e (взаимно простой с $\Psi(n)$).
- Находится закрытый ключ d: $d = e^{-1}(mod\Psi(n)$.
- *Открытый ключ*: (e, n). *Закрытый ключ*: (d, n).

2.6 Алгоритм схемы цифровой подписи RSA. Генерация ключей и хэш сообщения

1. Генерация ключей

- Выбираются большие простые числа p и q.
- Вычисляется модуль $n = p \cdot q$ и функция Эйлера $\Psi(n)$.
- Выбирается открытый ключ e (взаимно простой с $\Psi(n)$).
- Находится закрытый ключ d: $d = e^{-1}(mod\Psi(n)$.
- *Открытый ключ*: (e, n). *Закрытый ключ*: (d, n).

2. Хэширование сообщения

2.6 Алгоритм схемы цифровой подписи RSA. Генерация ключей и хэш сообщения

1. Генерация ключей

- Выбираются большие простые числа p и q.
- Вычисляется модуль $n = p \cdot q$ и функция Эйлера $\Psi(n)$.
- Выбирается открытый ключ e (взаимно простой с $\Psi(n)$).
- Находится закрытый ключ d: $d = e^{-1}(mod\Psi(n)$.
- *Открытый ключ*: (e, n). *Закрытый ключ*: (d, n).

2. Хэширование сообщения

- Отправитель вычисляет хэш сообщения $D = H(m)$.

2.7 Алгоритм схемы цифровой подписи RSA. Генерация ключей

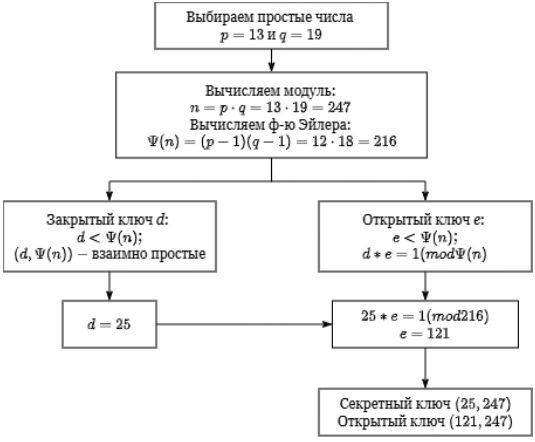


Рисунок 1: Пример генерации ключей

2.8 Алгоритм схемы цифровой подписи RSA. Подпись и проверка

3. Подпись закрытым ключом

2.8 Алгоритм схемы цифровой подписи RSA. Подпись и проверка

3. Подпись закрытым ключом

- Отправитель шифрует хэш закрытым ключом: $S = D^d mod n$.

2.8 Алгоритм схемы цифровой подписи RSA. Подпись и проверка

3. Подпись закрытым ключом

- Отправитель шифрует хэш закрытым ключом: $S = D^d mod n$.
- Подпись прикрепляется к исходному сообщению.

2.8 Алгоритм схемы цифровой подписи RSA. Подпись и проверка

3. Подпись закрытым ключом

- Отправитель шифрует хэш закрытым ключом: $S = D^d mod n$.
- Подпись прикрепляется к исходному сообщению.

4. Передача данных

2.8 Алгоритм схемы цифровой подписи RSA. Подпись и проверка

3. Подпись закрытым ключом

- Отправитель шифрует хэш закрытым ключом: $S = D^d mod n$.
- Подпись прикрепляется к исходному сообщению.

4. Передача данных

- Получатель получает пару: (m, S).

2.8 Алгоритм схемы цифровой подписи RSA. Подпись и проверка

3. Подпись закрытым ключом

- Отправитель шифрует хэш закрытым ключом: $S = D^d mod n$.
- Подпись прикрепляется к исходному сообщению.

4. Передача данных

- Получатель получает пару: (m, S).

5. Проверка открытым ключом

2.8 Алгоритм схемы цифровой подписи RSA. Подпись и проверка

3. Подпись закрытым ключом

- Отправитель шифрует хэш закрытым ключом: $S = D^d mod n$.
- Подпись прикрепляется к исходному сообщению.

4. Передача данных

- Получатель получает пару: (m, S).

5. Проверка открытым ключом

- Получатель расшифровывает подпись открытым ключом: $D' = S^e mod n$.

2.8 Алгоритм схемы цифровой подписи RSA. Подпись и проверка

3. Подпись закрытым ключом

- Отправитель шифрует хэш закрытым ключом: $S = D^d mod n$.
- Подпись прикрепляется к исходному сообщению.

4. Передача данных

- Получатель получает пару: (m, S).

5. Проверка открытым ключом

- Получатель расшифровывает подпись открытым ключом: $D' = S^e mod n$.
- Получатель самостоятельно вычисляет D и сравнивает с D'.

2.8 Алгоритм схемы цифровой подписи RSA. Подпись и проверка

3. Подпись закрытым ключом

- Отправитель шифрует хэш закрытым ключом: $S = D^d mod n$.
- Подпись прикрепляется к исходному сообщению.

4. Передача данных

- Получатель получает пару: (m, S).

5. Проверка открытым ключом

- Получатель расшифровывает подпись открытым ключом: $D' = S^e mod n$.
- Получатель самостоятельно вычисляет D и сравнивает с D'.
- Если совпадают - подпись действительна.

2.9 Алгоритм схемы цифровой подписи RSA. Подпись и проверка

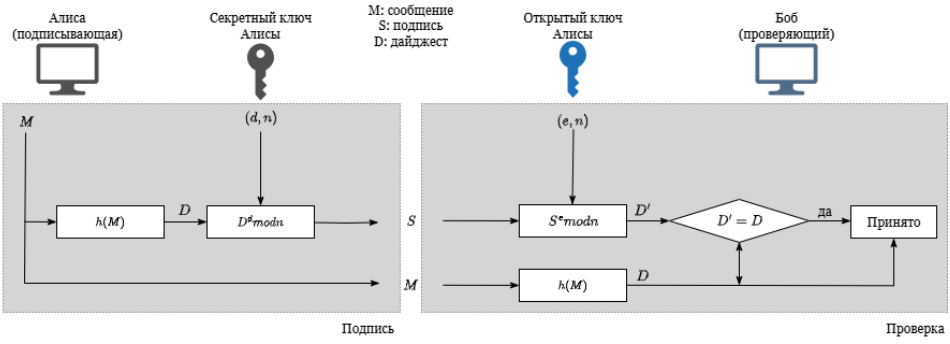


Рисунок 2: Алгоритм подписи и проверки

2.10 Алгоритм схемы цифровой подписи RSA. Подпись

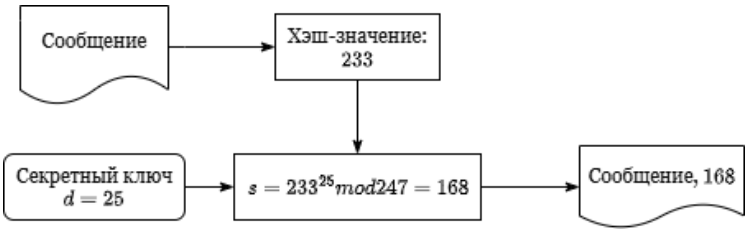


Рисунок 3: Алгоритм подписи. Пример

2.11 Алгоритм схемы цифровой подписи RSA. Проверка

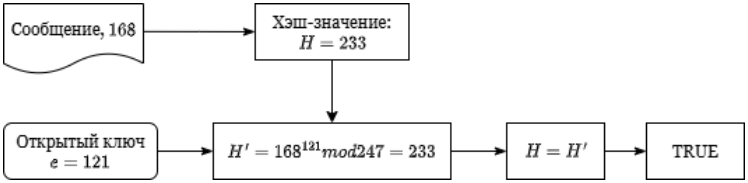


Рисунок 4: Алгоритм проверки. Пример

2.12 Атаки подписи RSA

1. *Атака только на ключ*

2.12 Атаки подписи RSA

1. *Атака только на ключ*

- Ева имеет лишь доступ к открытому ключу Алисы. Перехватив пару (M, S), пытается создать новое сообщение M', такое что:

$$M' = S^e mod n$$

2.12 Атаки подписи RSA

1. *Атака только на ключ*

- Ева имеет лишь доступ к открытому ключу Алисы. Перехватив пару (M, S), пытается создать новое сообщение M', такое что:

$$M' = S^e mod n$$

2. *Атака при известном сообщении*

2.12 Атаки подписи RSA

1. *Атака только на ключ*

- Ева имеет лишь доступ к открытому ключу Алисы. Перехватив пару (M, S), пытается создать новое сообщение M', такое что:

$$M' = S^e mod n$$

2. *Атака при известном сообщении*

- Ева использует мультипликативное свойство RSA. Перехватив две пары (M_1, S_1) и (M_2, S_2), подписанные одним ключом, создает:

$$M_* = M_1 \cdot M_2 mod n$$

$$S_* = S_1 \cdot S_2 mod n$$

2.12 Атаки подписи RSA

1. *Атака только на ключ*

- Ева имеет лишь доступ к открытому ключу Алисы. Перехватив пару (M, S), пытается создать новое сообщение M', такое что:

$$M' = S^e mod n$$

2. *Атака при известном сообщении*

- Ева использует мультипликативное свойство RSA. Перехватив две пары (M_1, S_1) и (M_2, S_2), подписанные одним ключом, создает:

$$M_* = M_1 \cdot M_2 mod n$$

$$S_* = S_1 \cdot S_2 mod n$$

3. *Атака по выбранному сообщению*

2.12 Атаки подписи RSA

1. *Атака только на ключ*

- Ева имеет лишь доступ к открытому ключу Алисы. Перехватив пару (M, S), пытается создать новое сообщение M', такое что:

$$M' = S^e mod n$$

2. *Атака при известном сообщении*

- Ева использует мультипликативное свойство RSA. Перехватив две пары (M_1, S_1) и (M_2, S_2), подписанные одним ключом, создает:

$$M_* = M_1 \cdot M_2 mod n$$

$$S_* = S_1 \cdot S_2 mod n$$

3. *Атака по выбранному сообщению*

- Ева заставляет Алису подписать два легитимных сообщения M_1 и M_2

2.13 Выводы

Было сформировано целостное представление о схеме цифровой подписи RSA.

2.14 Вопросы и ответы

Спасибо за внимание!