НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ім. Ігоря СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Звіт з виконання комп’ютерного практикуму

ДОСЛІДЖЕННЯ МЕТОДІВ РЕАЛІЗАЦІЇ СЛІПОГО ЦИФРОВОГО ПІДПИСУ

Виконали студенти
групи ФІ-32мн
Костюк Кирило,
Панасюк Єгор,
Пелешенко Любов

Перевірили: Селюх П.В.

Київ — 2023

Мета роботи: Дослідити можливість реалізації криптографічного протоколу сліпого підпису. Порівняти ефективність роботи різних можливих реалізацій сліпого цифрового підпису
Постановка задачі: Розглянути та порівняти між собою алгоритми реалізації сліпого цифрового підпису: Rsa реалізація та за схемою Шнорра. Описати переваги та недоліки, можливі атаки на ці протоколи.

ХІД РОБОТИ

Цифровий підпис: визначення та цілі

Цифровий підпис (ЦП) представляє собою математичний метод, який використовується для перевірки автентичності та цілісності цифрового документа, повідомлення чи програмного забезпечення. Цей метод є цифровим аналогом власноручного підпису або печатки, проте надає вищий рівень безпеки. Дійсний цифровий підпис у повідомленні гарантує одержувачеві, що воно походить від відомого відправника.

Цифрові підписи входять у склад більшості криптографічних протоколів і застосовуються у різних сферах, таких як розповсюдження програмного забезпечення, фінансові транзакції, управління контрактами та інші випадки, де важливо виявити підробку чи втручання.

Основні мети та завдання цифрового підпису включають:

- Підтвердження цілісності повідомлення.
- Підтвердження автентичності джерела, тобто автора повідомлення.
- Забезпечення невзможності підробки цифрового підпису.
- Забезпечення невзможності відмови підписника від підписаного повідомлення.
- Можливість багаторазової перевірки повідомлення різними користувачами у різний час без зміни криптосистеми.
- Юридична значимість.

Сліпий цифровий підпис: особливості та застосування

Унікальність сліпого цифрового підпису полягає в тому, що особа, яка підписує, не має інформації про зміст повідомлення, яке вона підписує. Термін "сліпий підпис" був введений Д. Шаумом у 1982 році, і він представив першу реалізацію цього типу підпису на основі

криптосистеми RSA. Безпека сліпого підпису ґрунтується на складності факторизації великих складених чисел.

Основна ідея сліпого підпису включає наступне:

1. Відправник A шифрує документ і відправляє його стороні B.
2. Сторона B, не знаючи змісту документа, підписує його і повертає назад стороні A.
3. Сторона A розшифровує документ, залишаючи на ньому лише підпис сторони B.

Після завершення цього протоколу сторона B не має інформації про повідомлення m, але може перевірити підпис з обмеженими знаннями про його вміст. Часто сліпий цифровий підпис порівнюють з виборчим процесом, де виборець вкладає анонімний бюлетень у конверт і передає його для підпису, не розглядаючи вмісту.

Головною метою сліпого цифрового підпису є запобігання підписуючій стороні B доступу до інформації, яку вона підписує, та відповідного підпису до цього повідомлення. Таким чином, підписане повідомлення залишається анонімним відносно сторони A.

Безпечна схема сліпого цифрового підпису повинна відповідати трьом властивостям:

1) **Нульове розголошення:** користувач може отримати підпис для даного повідомлення, не розкриваючи самого повідомлення підписуючій стороні.
2) **Невідстежуваність:** підписуюча сторона не може відстежувати пару підпис-повідомлення після оприлюднення підпису на повідомленні.
3) **Непідкладність:** лише підписуюча сторона може генерувати дійсний підпис.

Завдяки властивостям нульового розголошення та невідстежуваності, схема сліпого цифрового підпису може знаходити

широке застосування в областях, де необхідна конфіденційність, таких як системи електронного голосування.

Сліпий цифровий підпис на основі RSA

Припустимо, що A має відкриті параметри RSA (n, e) та секретний ключ d, а також нехай M - повідомлення від користувача B, де $M < n$.

Мета сліпого цифрового підпису полягає в тому, щоб A міг підписати повідомлення M, не маючи жодної інформації про його зміст (іншими словами, A не повинен мати можливість прочитати повідомлення). Алгоритм формування сліпого цифрового підпису на основі RSA виглядатиме наступним чином:

1. Аліса вибирає випадковий маскуючий множник r, взаємно простий з p, і обчислює $m' \equiv mr^e \mod p$.
2. Аліса відсилає m' по відкритому каналу Бобу.
3. Боб обчислює $s' \equiv (m')^d \mod p$, використовуючи свій закритий ключ(p, d).
4. Боб відсилає s' назад Алісі.
5. Аліса прибирає своє початкове маскування і отримує підписане Бобом вихідне повідомлення m наступним чином: $s \equiv s' * r^{-1} \mod p \equiv m^d \mod p$.

Таким чином формується повідомлення (M, S) зі сліпим цифровим підписом.

Сліпий підпис з використанням ЕЦП Шнорра

Якщо Аліса бажає підписати повідомлення m для Боба так, щоб, по-перше, Боб не міг прочитати повідомлення під час підпису, і, по-друге, Боб не зміг би визначити особу, яка ініціювала протокол сліпого підпису для конкретного повідомлення m під час його отримання, то протокол може бути виконаний за наступним чином:

1. Аліса ініціює взаємодію з Бобом.
2. Боб відправляє Алісі значення $R = a^k \mod p$.
3. Аліса обчислює значення$R' = Ra^{-w}y^{-t} \mod y$ (w і t — випадкові числа, що не перевищують y), $E' = H(m||R')$ і $E = E' + t \mod y$, після чого відправляє Бобу значення E.
4. Боб обчислює значення S, таке що $R = a^S y^E \mod p$, і відправляє S Алісі.
5. Аліса обчислює підпис (E', S'), де $E' = E^{-t} \mod y$ і $S' = S - w \mod y$, яка є справжньою по відношенню до повідомлення m[8].

Уразливості сліпого підпису

Алгоритм RSA може бути підданий атакам, що дозволяють розшифрувати раніше сліпо підписане повідомлення, видаючи його за повідомлення, яке ще не було підписане. Оскільки процес підпису є еквівалентним розшифруванню підписуючою стороною (з використанням секретного ключа), атакуючий може підставити для підпису вже підписану сліпу версію повідомлення m, зашифрованого з використанням відкритого ключа підписуючої сторони, іншими словами, він може підмінити повідомлення m'.

$$\begin{aligned} m'' &= m'r^e \pmod{n} \\ &= (m^e \pmod{n} \cdot r^e) \pmod{n} \\ &= (mr)^e \pmod{n} \end{aligned}$$

де m' — це зашифрована версія повідомлення. Коли повідомлення підписане, відкритий текст m легко отримуємо:

$$\begin{aligned} s' &= m''^d \pmod{n} \\ &= ((mr)^e \pmod{n})^d \pmod{n} \\ &= (mr)^{ed} \pmod{n} \\ &= m \cdot r \pmod{n}, \text{since } ed \equiv 1 \pmod{\phi(n)} \end{aligned}$$

де $\phi(n)$ — це Функція Ейлера. Тепер повідомлення легко отримати.

$$m = s' \cdot r^{-1} \pmod{n}$$

Атака успішна через те, що в даній схемі підписуюча сторона непосредствено підписує саме повідомлення, в той час як у звичайних схемах підпису підписуюча сторона, наприклад, підписує криптографічний хеш-функції. Таким чином, через мультиплікативну властивість RSA, один і той же ключ не повинен використовуватися одночасно для шифрування і сліпого підпису.

Порівняння алгоритмів сліпого цифрового підпису на основі RSA і Шнорра. Проблематика реалізації

Нам вдалося реалізувати алгоритм сліпого підпису на основі RSA, і ця реалізація є досить простою за умови наявності бібліотеки, яка підтримує велику арифметику та швидке піднесення до великого ступеня числа за модулем. Наприклад, наша реалізація, використовуючи бібліотеку BigInteger, виконується за 4,2 * 10^(-9) секунд, при цьому утворення маски вимагає всього 0,2 * 10^(-9) секунди. Оцінки отримані для чисел довжиною 1024 біта. Незважаючи на те, що цей алгоритм є простим для реалізації і

ефективним в обчислювально обмежених ресурсах, слід врахувати ризик атаки, згаданої вище.

Алгоритм Шнорра виявився менш простим для реалізації, особливо під час генерації ключів, оскільки потрібно створити прості числа p та q, де $q|p - 1$, і обрати $a \in Zp$ так, щоб $a^q = 1 \bmod p$ і $a \neq 1$. Ми вирішили спочатку генерувати q за допомогою Блюм-Блюма-Шуба, перевіряти його на простоту, а якщо воно є простим - генерувати другий множник для отримання $p - 1$. Однак найбільшою трудністю було знайти генератор або елемент порядку q, оскільки обчислення його в групі з великим порядком є обчислювально складною задачею. Ясно, що якщо $p \geqslant 2^{512}$, то перебір всіх елементів групи не має сенсу, а отримання генератора або елементу з порядком q також виявляється проблематичним.

ВИСНОВКИ

У даній роботі ми дослідили можливість реалізації алгоритмів сліпого підпису, таких як RSA та Шнорра. Реалізація алгоритму RSA може бути успішною при наявності бібліотек для багаторозрядної арифметики та виявляється досить простою для побудови. Основним недоліком цього алгоритму є можливість атаки, використовуючи шифротекст замість повідомлення.

Алгоритм Шнорра, навпаки, виявився стійким до цієї атаки, оскільки використовує гешування повідомлення. Однак для його реалізації існує серйозний недолік, пов'язаний із пошуком елемента великого порядку під час генерації ключів.