АСИМЕТРИЧНІ КРИПТОСИСТЕМИ ТА ПРОТОКОЛИ
КОМП'ЮТЕРНИЙ ПРАКТИКУМ №3

Криптосистема Рабіна
Атака на протокол доведення знання без розголошення

1. Мета та основні завдання роботи

Ознайомлення із криптосистемою Рабіна та особливостям її реалізації. Ознайомлення з криптографічними протоколами взагалі та протоколами доведення знання без розголошення зокрема. Ознайомлення із перевагами, недоліками та особливостями реалізації різних криптографічних протоколів. Аналіз наведеного протоколу; реалізація атаки на цей протокол.

2. Основні теоретичні відомості

2.1. Криптосистема Рабіна

Криптосистема Рабіна була запропонована як перша асиметрична криптосистема із доказовою стійкістю. Вона ґрунтується на використанні важкооборотної функції Рабіна $f(x) = x^2 \bmod n$, де $n = pq$, обертання якої еквівалентно факторизації числа n. Система Рабіна включає в себе як схему шифрування, так і схему цифрового підпису. Опишемо їх більш детально.

Генерування ключів

Аліса генерує два великі прості числа p, q, кожне виду $4k+3$, та обчислює $n = pq$ (прості числа такого виду називаються *простими числами Блюма*, а число n – *числом Блюма*). Числа p, q є секретним ключем Аліси, а число n – її відкритим ключем.

У розширеній схемі Рабіна також використовується додаткове число $b \in Z_n$, яке включається в обидва ключі.

Форматування повідомлень

Відкриті повідомлення, шифротексти та цифрові підписи у схемі Рабіна є елементами кільця Z_n. Втім, до відкритих текстів m висувається обмеження $m > \sqrt{n}$, щоб, наприклад, запобігти дешифруванню шляхом звичайного знаходження арифметичного квадратного кореня. Для виконання цього обмеження в схемі Рабіна використовують форматування вхідних повідомлень.

У даному комп'ютерному практикумі пропонується використовувати таку процедуру форматування вхідних повідомлень.

Нехай l – це кількість байтів, необхідних для двійкового запису числа n. Вхідне повідомлення m повинно мати довжину, яка не перевищує $l-10$ байтів. Форматування відбувається в такий спосіб: генерується випадкове 64-бітове число $r \in Z_{2^{64}}$ та обчислюється число

$$x = 255 \cdot 2^{8(l-8)} + m \cdot 2^{64} + r.$$

Число x є форматованим повідомленням m. Іншими словами, повідомлення m доповнюється додатковими байтами таким чином:

$$x \leftarrow \underbrace{0x00}_{1\,байт} \| \underbrace{0xFF}_{1\,байт} \| \underbrace{m}_{(l-10)\,байтів} \| \underbrace{r}_{8\,байтів}.$$

Схема шифрування Рабіна

Опишемо спочатку процедуру зашифрування.

Нехай n – відкритий ключ Аліси, $x \in Z_n$ – відформатоване повідомлення, яке треба зашифрувати для Аліси. Боб виконує наступні обчислення:

$$y = x^2 \bmod n,$$
$$c_1 = x \bmod 2,\ c_2 = \left[\left(\frac{x}{n}\right) = 1\right],$$

де квадратні дужки є *символом Айверсона* (індикаторною функцією), тобто $c_2 = 1$, якщо символ Якобі $\left(\frac{x}{n}\right) = 1$, і $c_2 = 0$, якщо символ Якобі $\left(\frac{x}{n}\right) \neq 1$.

Шифротекстом є трійка (y, c_1, c_2). Біти c_1 (біт парності) та c_2 (символ Якобі) є додатковою інформацією, необхідною для коректного розшифрування.

У розширеній схемі Рабіна шифротекст обчислюється за формулою:

$$y = x(x+b) \bmod n,$$
$$c_1 = \left(\left(x + \frac{b}{2}\right) \bmod n\right) \bmod 2,\ c_2 = \left(\frac{x + \frac{b}{2}}{n}\right).$$

Перейдемо до опису процедури розшифрування.

Одержавши шифротекст (y, c_1, c_2), Аліса обчислює чотири квадратні корені $\sqrt{y} \bmod n$. Коректним відкритим текстом x буде той корінь, для якого співпадуть обидва додаткові біти шифротексту: біт парності та символ Якобі. Для одержання правильного відкритого тексту m Аліса повинна видалити байти форматування (перевіривши перед цим їх коректність).

У розширеній схемі Рабіна шифротекст шукається за формулою

$$x = \left(-\frac{b}{2} + \sqrt{y + \frac{b^2}{4}}\right) \bmod n.$$

Знов-таки, серед чотирьох можливих варіантів обирається той, для якого співпадають обидва додаткові біти.

Схема цифрового підпису Рабіна

Процедура постановки цифрового підпису у схемі Рабіна виглядає так.

а) Аліса форматує вхідне повідомлення m у повідомлення x.

б) Аліса перевіряє, чи є x квадратичним лишком за модулем n, тобто чи виконуються рівності

$$\left(\frac{x}{p}\right)=\left(\frac{x}{q}\right)=1.$$

Якщо x не є квадратичним лишком за модулем n, Аліса повертається до п. а) та виконує переформатування із іншим числом r.

в) Аліса обчислює чотири квадратні корені $\sqrt{x} \bmod n$ та обирає один з них навмання як цифровий підпис s під повідомленням m.

Для перевіряння підписаного повідомлення (m, s) Боб просто обчислює значення $x' = s^2 \bmod n$ та перевіряє, чи є x' відформатованим повідомленням m.

2.2. Швидке обчислення квадратних коренів за модулями Блюма

Найскладнішою обчислювальною операцією у криптосистемі Рабіна є знаходження квадратних коренів за модулем. У випадку, коли модуль є числом Блюма, можна пришвидшити обчислення коренів за рахунок властивостей таких чисел.

Нехай потрібно розв'язати рівняння $x^2 \equiv y \pmod n$, де $n = pq$, і p, q – різні прості числа виду $4k+3$ кожне.

а) Обчислюються значення

$$s_1 = y^{\frac{p+1}{4}} \bmod p,\ s_2 = y^{\frac{q+1}{4}} \bmod q.$$

б) За розширеним алгоритмом Евкліда знаходяться такі числа u, v, що $up + vq = 1$.

в) Чотири корені рівняння обчислюються із співвідношення $x = \pm ups_1 \pm vqs_2$ (кожна пара знаків відповідає одному кореню).

2.3. Протоколи доведення без розголошення

Основну задачу, яку повинні розв'язувати протоколи доведення без розголошення, проілюструємо на такому прикладі.

Нехай n є числом Блюма, тобто $n = pq$, де $p, q \equiv 3 \pmod 4$, і Боб знає розклад n на прості множники. Він намагається довести це Алісі, але при цьому не хоче, щоб Аліса також дізналась про значення p та q. В той же час Аліса хоче бути впевненою, що Боб її не обдурює. Вони домовляються, що Боб надасть Алісі деяку іншу інформацію за її вибором, яку Боб може одержати тільки знаючи p та q. Таким чином, Аліса впевниться у правоті Боба, а Боб не розголосить важливу для нього інформацію.

Будь-який протокол доведення без розголошення повинен мати такі властивості:

1) *Повнота:* якщо твердження, яке доводиться, дійсно вірне, то Боб (той, що доводить) переконає в цьому Алісу (того, хто перевіряє).

2) *Коректність:* якщо твердження, яке доводиться, невірне, то Боб не може переконати Алісу в тому, що твердження вірне, навіть якщо він буде діяти нечесно.

3) *Нульове розголошування:* якщо твердження вірне, то Аліса не зможе дізнатись нічого, окрім самого факту, що твердження вірне, навіть якщо буде діяти нечесно.

2.4. Протокол доведення знання розкладу числа на прості множники

Нехай Боб знає розклад числа Блюма $n = pq$ та хоче переконати в цьому Алісу, яка знає лише число n. Вони домовляються про такий порядок дій:

1. Аліса обирає випадкове число x та надсилає Бобові число $y = x^4 \bmod n$.
2. Боб, знаючи p та q, обчислює квадратні корені $\sqrt{y} \bmod n$ та обирає в якості числа $z = \sqrt{y} \bmod n$ той корінь, який є квадратичним лишком за модулем n. Число z Боб надсилає Алісі.
3. Аліса перевіряє, чи дійсно $z = x^2 \bmod n$. Якщо рівність вірна, то Аліса впевнюється, що Боб знає розклад n на прості множники.

Наведений протокол є двораундовим: Аліса та Боб використовують усього два акти надсилання даних. Однак було доведено, що для виконання всіх властивостей протоколи доведення без розголошення повинні мати щонайменше три раунди, а тому даний протокол повинен бути нестійким. І дійсно, хоча цей протокол є повним та коректним, він не забезпечує нульове розголошення.

Опишемо атаку на наведений протокол.

Нехай n є числом Блюма (тобто множники p та q мають вигляд $4k+3$). Тоді злонамірна Аліса може викрити таємниці Боба, якщо буде діяти за таким алгоритмом.

1) Аліса обирає випадкове t та надсилає Бобові число $y = t^2 \bmod n$.
2) Чесний Боб надсилає Алісі z – той квадратний корінь з y, який є квадратичним лишком.
3) З імовірністю приблизно 0.5 Аліса матиме $t \neq \pm z$, звідки вона знатиме, що найбільший спільний дільник $\gcd(t+z, n)$ дорівнюватиме p або q.

3. Порядок і рекомендації щодо виконання роботи

Комп'ютерний практикум включає в себе два завдання: реалізацію розширеної криптосистеми Рабіна та реалізацію атаки на описаний протокол доведення із нульовим розголошенням.

Реалізація криптосистеми Рабіна виконується таким саме чином, як і реалізації криптосистеми RSA у комп'ютерному практикумі №2. Основні операції (генерування ключів, шифрування/розшифрування, постановка/перевірка підпису) необхідно оформлювати високорівневими процедурами GenerateKeyPair(), Encrypt(), Decrypt(), Sign(), Verify().

Кожну операцію рекомендується перевіряти шляхом взаємодії із тестовим середовищем, розташованим за адресою

http://asymcryptwebservice.appspot.com/?section=rabin .

Наприклад, для перевірки коректності операції шифрування необхідно а) зашифрувати власною реалізацією повідомлення для серверу та розшифрувати його на сервері, б) зашифрувати на сервері повідомлення для вашої реалізації та розшифрувати його локально.

Для проведення атаки на протокол доведення із нульовим розголошенням також необхідно користуватись тестовим середовищем.

За адресою http://asymcryptwebservice.appspot.com/?section=znp проживає сервер, який генерує ключі RSA довжиною 2048 біт та користується описаним протоколом, щоб довести будь-кому своє знання розкладу модуля на прості множники.

1. Реалізуйте допоміжне програмне забезпечення для проведення сценарію атаки.

2. Згенеруйте на сервері ключі для аналізу. Сервер поверне вам значення модуля n (це значення буде існувати доти, доки ви не завершите сесію зв'язку).

3. Користуючись формою введення, надсилайте серверу випадкові t, поки атака не завершиться успіхом. Зафіксуйте, з якої спроби вам вдалось зламати ключ.

4. Продемонструйте викладачеві вашу перемогу над бездушною машинерією.

4. Оформлення звіту

Звіт до комп'ютерного практикуму оформлюється згідно зі стандартними правилами оформлення наукових робіт, за такими винятками:

- дозволяється використовувати шрифт Times New Roman 12pt та одинарний інтервал між рядками;
- для оформлення фрагментів текстів програм дозволяється використовувати шрифт Courier New 10pt та друкувати тексти в дві колонки;
- дозволяється не починати нові розділи з окремої сторінки.

До звіту можна не включати анотацію, перелік термінів та позначень та перелік використаних джерел. Також не обов'язково оформлювати зміст.

Звіт має містити:

- мету лабораторної роботи;
- постановку задачі та варіант завдання;
- хід роботи, опис труднощів, що виникали, та шляхів їх розв'язання;
- значення вибраних чисел p, q, із зазначенням кандидатів, що не пройшли тест перевірки простоти, ключів і параметрів розширеної криптосистеми Рабіна для абонентів A і B;
- чисельні значення прикладів відкритого тексту, шифротексту, цифрового підпису у схемі Рабіна для A і B;
- значення модуля n, згенероване сервером;
- покрокову реалізацію сценарію атаки на протокол, із зазначенням усіх проміжних значень;
- перевірку, що ви дійсно знайшли розклад n на прості множники;
- висновки.

Тексти всіх програм здаються викладачеві в електронному вигляді для перевірки на плагіат. До захисту комп'ютерного практикуму допускаються студенти, які оформили звіт та пройшли перевірку програмного коду.

5. Контрольні питання

1) Яким чином обчислюються квадратні корені за простим модулем?

2) Яким чином обчислюються квадратні корені за модулем виду $n = pq$? Обґрунтуйте коректність наведеного у п. 2.2 алгоритму обчислення квадратних коренів.

3) Опишіть просту та розширену схеми Рабіна: процедури генерування ключів, шифрування, розшифрування, постановки та перевірки підпису.

4) З якою метою використовується попереднє форматування відкритих текстів у схемі Рабіна?

5) Які задачі розв’язують протоколи доведення без розголошення?

6) Які властивості повинен мати протокол доведення без розголошення?

7) Доведіть, що наведений в даному практикумі протокол є повним.

8) Доведіть, що наведений в даному практикумі протокол є коректним.

9) Чому для коректної реалізації даного протоколу потрібно, щоб модуль n був числом Блюма?

10) Чому в запропонованій атаці імовірність одержати $t \neq z$ дорівнює 0.5?

11) Скільки в середньому потрібно зробити запитів до сервера в описаному сценарії атаки для її успішної реалізації?

12) Чому якщо $t \neq z$, то $\gcd(t+z, n)$ дорівнює p або q?

6. Оцінювання комп’ютерного практикуму

За виконання лабораторної роботи студент може одержати до 11 рейтингових балів; зокрема, оцінюються такі позиції:

– реалізація програм – до чотирьох балів (в залежності від правильності та швидкодії);

– теоретичний захист роботи – до шести балів;

– своєчасне виконання роботи – 1 бал;

– несвоєчасне виконання роботи – (-1) бал за кожен тиждень пропуску.

Програмний код, створений під час виконання комп’ютерного практикуму, перевіряється на наявність неправомірних запозичень (плагіату) за допомогою сервісу *Stanford MOSS Antiplagiarism*. У разі виявлення в програмному коді неправомірних запозичень реалізація програм оцінюється у 0 балів, а за виконання практикуму студент одержує штраф (–10) балів.

Студенти допускаються до теоретичного захисту тільки за умови оформленого звіту з виконання практикуму.