

# АСИМЕТРИЧНІ КРИПТОСИСТЕМИ ТА ПРОТОКОЛИ

## КОМП'ЮТЕРНИЙ ПРАКТИКУМ №3

### Атака на протокол доведення знання без розголошення

#### 1. Мета та основні завдання роботи

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. Протоколи доведення без розголошення

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

Нехай  $n$  є числом Блума, 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 розголошення*: якщо твердження вірне, то Аліса не зможе дізнатись нічого, окрім самого факту, що твердження вірне, навіть якщо буде діяти нечесно.

##### 2.2. Протокол доведення знання розкладу числа на прості множники

Нехай Боб знає розклад  $n = pq$  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.

### 2.3. Атака 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 такою схемою.

- 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  $t \neq z$ , звідки вона знатиме, що найбільший спільний дільник  $\gcd(t + z, n)$  дорівнюватиме  $p$  або  $q$ .

### 3. Порядок і рекомендації щодо виконання роботи

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

1. Згенеруйте на сервері ключі для аналізу. Сервер поверне вам значення модуля  $n$  (це значення буде існувати доти, доки ви не завершите сесію зв'язку).
2. Реалізуйте допоміжне програмне забезпечення для проведення сценарію атаки.
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 текстів програм дозволяється використовувати шрифт Courier New 10pt та друкувати тексти в дві колонки;
- дозволяється не починати нові розділи з окремої сторінки.

Звіт має містити:

1. Мету лабораторної роботи
2. Постановку задачі та варіант завдання
3. Хід роботи, опис труднощів, що виникали, та шляхів їх розв'язання.
4. Ваш унікальний ідентифікатор та значення модуля  $n$ , згенероване сервером.
5. Покрокову реалізацію сценарію атаки на протокол, із зазначенням усіх проміжних значень.
6. Перевірку, що ви дійсно знайшли розклад  $n$  на прості множники.
7. Висновки.
8. Тексти всіх програм.

## 5. Контрольні питання

- 1) Які задачі розв'язують протоколи доведення без розголошення?
- 2) Які властивості повинен мати протокол доведення без розголошення?
- 3) Доведіть, що наведений в даному практикумі протокол є повним.
- 4) Доведіть, що наведений в даному практикумі протокол є коректним.
- 5) Яким чином обчислюються квадратні корені за простим модулем?
- 6) Яким чином обчислюються квадратні корені за модулем виду  $n = pq$ ?
- 7) Чому для коректної реалізації даного протоколу потрібно, щоб модуль  $n$  був числом Блюма?
- 8) Чому в запропонованій атаці імовірність одержати  $t \neq z$  дорівнює 0.5?
- 9) Скільки в середньому потрібно зробити запитів до сервера в описаному сценарії атаки для її успішної реалізації?
- 10) 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 12 рейтингових балів; зокрема, оцінюються такі позиції:

- реалізація програм – до чотирьох балів (в залежності від правильності та швидкодії);
- оформлення звіту – 1 бал;
- теоретичний захист роботи – до шести балів;
- своєчасне виконання роботи – 1 бал;
- несвоєчасне виконання роботи – (-2) бали за кожні два тижні пропуску.