УДК 004.738.5

АСИМЕТРИЧНІ КРИПТОГРАФІЧНІ СИСТЕМИ

Данов Артем

Науковий керівник: канд. пед. наук Ганжела С.І.

Центральноукраїнський державний педагогічний університет імені Володимира Винниченка, м. Кропивницький, Україна

В статті висвітлюються основні проблеми захисту інформації та розглядаються асиметричні криптографічні системи. В ході дослідження проаналізовано асиметричні криптографічні системи як один з найбільш перспективних напрямків розвитку електронних систем захисту даних. Докладно розглянуто алгоритм RSA як типовий представник сімейства асиметричних шифрів. З цією метою алгоритм реалізовано засобами ***C++.***

Ключові слова: асиметричні алгоритми, криптографія, захист інформації, криптографічний алогоритм.

ASYMMETRIC ENCRYPTION

A. Danov

Scientific supervisor: Candidate of Pedagogical Sciences Ganzhela S.I.

The Volodymyr Vynnychenko Central Ukrainian State Pedagogical University, Kropyvnytsky, Ukraine

In this article showing the main problems of information protection and examined asymmetric encryption. In the process of explore has been analyzed asymmetric encryption as one of the most promising areas for the development of electronic data protection systems. In detail examined the RSA algorithm as a typical representative of the family of asymmetric ciphers. And because of it the algorithm implemented by programing language C ++.

Key words: asymmetric algorithms, cryptography, protection of information, cryptographic algorithm.

Постановка проблеми. На сучасному етапі розвитку науки та техніки все більше уваги приділяється безпеці передачі інформації, збереженні її секретності, розробці державних стандартів з захисту інформації.

Розвиток нових інформаційних технологій і загальна комп'ютеризація призвели до тому, що інформаційна безпека не тільки стає обов'язковим атрибутом, вона ще й одна з важливих характеристик інформаційних систем. Існує досить великий клас систем обробки інформації, при розробці яких фактор безпеки відіграє першорядну роль (наприклад, банківські інформаційні системи).

Під безпекою інформаційних систем розуміється захищеність системи від випадкового або навмисного втручання в нормальний процес її функціонування, від спроб розкрадання (несанкціонованого отримання)

інформації, модифікації або фізичного руйнування її компонентів. Інакше кажучи, це здатність протидіяти різним впливам на інформаційну систему. Під загрозою безпеки інформації розуміються події або дії, які можуть призвести до спотворення, несанкціонованого використання або навіть до руйнування інформаційних ресурсів керованої системи, а також програмних і апаратних засобів. Тому питання розробки та удосконалення криптографічних систем є вельми актуальними.

На сьогоднішній день завдяки постійному застосуванню відкритих мереж передачі даних, таких як Internet, криптографічні протоколи знаходять все більш широке застосування для вирішення різноманітних кола завдань і забезпечення послуг, що надаються користувачам таких мереж.

Аналіз останніх досліджень і публікацій. Аналіз останніх досліджень і публікацій показав, що в останні роки науковці надають значної уваги різним аспектам проблеми захисту інформації. Так, головний редактор журналу "Сучасний захист інформації" С. Довбешко розглядав кіберзахист в Україні та розроблення рішень про ліквідацію наслідків кібератак на державні інформаційні ресурси фінансового сектору. Його колега М. Аріпов вказав, що при вирішенні кібербезпекових питань ми зможемо створити ефективну та дієву національну систему кібербезпеки. К. Бабенко запропонував новий метод класифікації шкідливого коду на основі послідовності викликів WinAPI і їх аргументів, а також файлів, які створюються аналізуючим додатком.

Постановка завдання. Метою статті є аналіз ефективності асиметричних криптографічних систем. З цією метою було досліджено алгоритм одного із стандарту шифрування даних, а саме RSA і створено систему, яка дозволяє шифрувати та розшифровувати текст за цим алгоритмом.

Асиметричні системи

Асиметричні системи також називають криптосистемами з відкритим ключем. Це такий спосіб шифрування даних, при якому відкритий ключ передається по відкритому каналу (не приховується) і використовується для

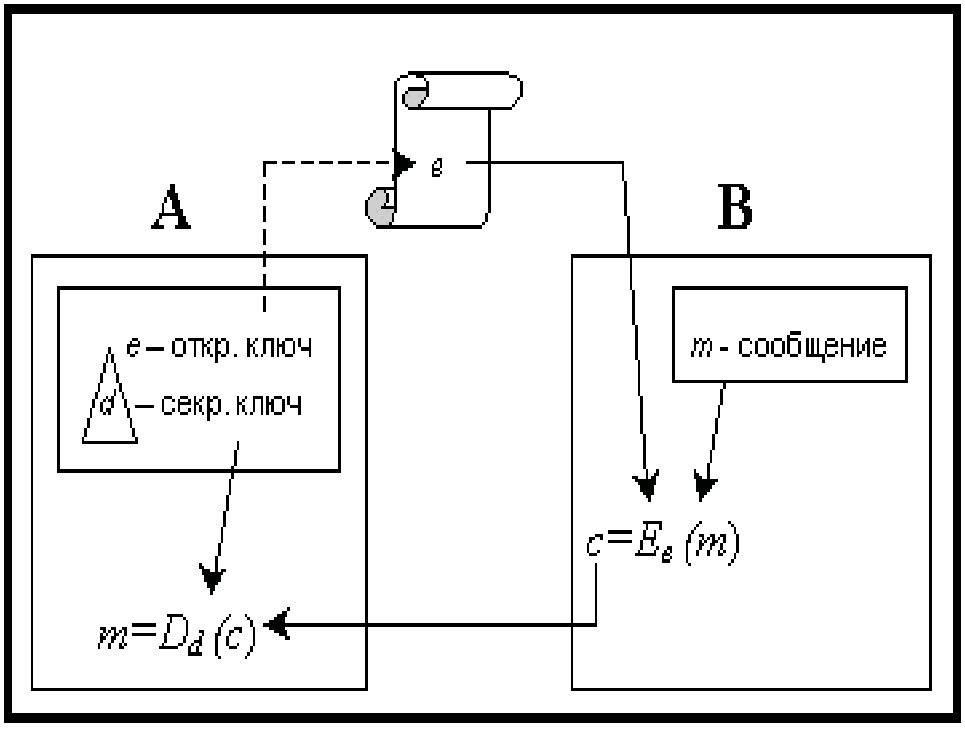
перевірки електронного підпису і для шифрування даних. Для дешифрування і створення електронного підпису використовується другий ключ, секретний.

Сам пристрій асиметричних криптосистем використовує ідею односторонніх функцій f (x), в яких нескладно знайти x, знаючи значення самої функції але майже неможливо знайти саму f (x), знаючи тільки значення x. Прикладом такої функції може служити телефонний довідник великого міста, в якому легко знайти номер людини, знаючи його прізвище та ініціали, але вкрай складно, знаючи номер, обчислити власника.

Принцип роботи асиметричних систем

Припустимо, є два абонента: A і B, і абонент B хоче відправити зашифроване повідомлення абоненту A. Він зашифровує повідомлення за допомогою відкритого ключа та передає його вже зашифрованим по відкритому каналу зв'язку. Отримавши повідомлення, абонент A починає його розшифрування за допомогою секретного ключа і читає.

При отриманні повідомлення абонент A повинен аутентифікувати свою особистість перед абонентом B для того, щоб віддалена особа не змогла видати себе за абонента A і підмінити його відкритий ключ своїм.



Приклади асиметричних шифрів

- **RSA** (Rivest-Shamir-Adleman, Ривест — Шамир — Адлеман)
- **DSA** (Digital Signature Algorithm)
- **Elgamal** (Шифросистема Эль-Гамаля)
- **ECC** (Elliptic Curve Cryptography, криптография эллиптической кривой)
- **ГОСТ Р 34.10-2001**
- **Rabin**
- **Luc**
- **McEliece**

Асиметричний шифр RSA

RSA (абревіатура від прізвищ Rivest, Shamir і Adleman) - криптографічний алгоритм з відкритим ключем, який базується на обчислювальної складності задачі факторизації великих цілих чисел.

Криптосистема RSA стала першою системою, придатною і для шифрування, і для цифрового підпису. Алгоритм використовується у великій кількості криптографічних додатків, включаючи PGP, S / MIME, TLS / SSL, IPSEC / IKE і інших.

Спочатку потрібно згенерувати відкритий і закриті ключі:

- Візьмемо два великих простих числа p and q.
- Визначимо n, як результат множення p на q $n = p * q$.

Виберемо випадкове число, яке назвемо d. Це число повинне бути взаємно простим (не мати жодного спільного дільника, крім 1) з результатом множення $p - 1 * (q - 1)$.

Визначимо таке число e, для якого є істинним наступне співвідношення

$e * d \ mod \ p - 1 * q - 1 = 1.$

Назвемо відкритим ключем числа e і n, а секретним $-d$ і n.

Для того, щоб зашифрувати дані з відкритого ключа $\{e, d\}$, необхідно наступне:

- розбити шифрований текст на блоки, кожен з яких може бути представлений у вигляді числа $M\ i\ = 0,1,2 \ldots, n-1$ (тобто тільки до $n-1$)
- зашифрувати текст, що розглядається як послідовність чисел $M\ (i)$ за формулою $C\ i\ =\ M\ I\ ^{e}\ mod\, n.$

Щоб розшифрувати ці дані, використовуючи секретний ключ $\{e, d\}$, необхідно виконати наступні обчислення: $M\ i\ =\ C\ I\ ^{d}\ mod\, n.$ В результаті буде отримано безліч чисел $M\ i$, які представляють собою вихідний текст.

Наступний приклад демонструє алгоритм шифрування RSA:

Зашифруємо і розшифруємо повідомлення "CAB" за алгоритмом RSA. Для простоти візьмемо невеликі числа - це зменшть час для наших розрахунків.

- Виберемо p = 3 and q = 11.
- Визначимо n = 3 * 11 = 33.
- Знайдемо $p-1\ *\ q-1\ = 20.$ Отже, d дорівнюватиме, наприклад, 3: $(d-3)$
- Виберемо число e за такою формулою: $e*3\ \ mod\, 20 = 1.$ Значить e дорівнюватиме, наприклад, 7: $e = 7$.
- Уявімо шифроване повідомлення як послідовність чисел у діапазоні від 0 до 32. Буква A = 1, B = 2, C = 3.

Тепер зашифровуємо повідомлення, використовуючу відкритий ключ {7,33}

- $C1 =\ 3^{7}\ \ mod\, 33 = 2187\, mod\, 33 = 9;$
- $C2 =\ 1^{7}\ \ mod\, 33 = 1\, mod\, 33 = 1;$
- $C3 =\ 2^{7}\ \ mod\, 33 = 128\, mod\, 33 = 29;$

Тепер розшифровуємо дані, використовуючи закритий ключ {3,33}.

- $M1 =\ 9^{3}\ \ mod\, 33 = 729\, mod\, 33 = 3(C);$
- $M2 =\ 1^{3}\ \ mod\, 33 = 1\, mod\, 33 = 1(A);$
- $M3 =\ 29^{3}\ \ mod\, 33 = 24389\, mod\, 33 = 2(B);$

Висновки.

У статті висвітлено загальні проблеми захисту інформації. В ході дослідження проаналізовано асиметричні криптографічні системи як один з найбільш перспективних напрямків розвитку електронних систем захисту даних. Докладно розглянуто алгоритм RSA як типовий представник сімейства асиметричних шифрів. Реалізація цього алгоритму засобами C++ довела його ефективність і перспективність подальших досліджень у цьому напрямку.

Список літератури

1. Алгоритм шифрования RSA [Електронний ресурс]. – Режим доступу до ресурсу: http://www.e-nigma.ru/stat/rsa
2. Сучасний захист інформації [Електронний ресурс] – Режим доступу до ресурсу: http://www.dut.edu.ua/ua/132-suchasniy-zahist-informacii-periodichni-vidannya
3. Криптография [Електронний ресурс] – Режим доступу до ресурсу: http://www.tadviser.ru/index.php/