УДК 51-7

АЛГЕБРАИЧЕСКИЕ ОСНОВЫ КРИПТОГРАФИИ

Никитин В.В.
Пермский государственный гуманитарно-педагогический университет,
Пермь, Россия

Аннотация
В статье приведена классификация криптосистем, рассмотрены основные математические понятия и теоремы, используемые при создании криптографических систем с открытыми ключами. Проанализирована проблема распределения ключей.

Ключевые слова: криптография, открытый ключ, защита информации, шифрование

ALGEBRAIC UNDERLIES CRYPTOGRAPHY

Nikitin V.V.
Perm State University of Humanities and Education,
Perm, Russia

Annotation

The article provides a classification of cryptosystems, the basic mathematical concepts and theorems used in the creation of cryptographic systems, public key. We analyzed the problem of the distribution of keys.

Keywords: cryptography, public key, information security, encryption.

С зарождением человеческой цивилизации возникла необходимость передачи информации одним людям так, чтобы она осталась тайной для других.

Существовали три основных способа защиты информации. Один из них предполагал защиту ее чисто силовыми методами: охрана документа (носителя информации) физическими лицами, передача его специальным курьером и т.д. Второй способ получил название "стеганография" (от *лат*. тайнопись). Он заключался в сокрытии самого факта наличия информации. В данном случае использовались так называемые симпатические чернила. При соответствующем "проявлении" бумаги текст становился видимым. Третий

способ защиты информации заключался в преобразовании смыслового текста в некий набор хаотических знаков (букв алфавита). Получатель данного донесения имел возможность преобразовать его в то же самое осмысленное сообщение, если обладал ключом к его построению. Этот способ защиты информации называется *криптографическим*.

Предметом криптографии является такое преобразование информации, при котором ее прочтение (восстановление) возможно только при знании ключа.

В качестве информации, подлежащей шифрованию и дешифрованию, будут рассматриваться тексты, построенные на некотором алфавите. Под этими терминами понимается следующее.

Текст - упорядоченный набор из элементов алфавита.

Шифрование - преобразовательный процесс исходного текста в шифрованный текст.

Дешифрование – обратный процесс шифрованию. На основе ключа шифрованный текст преобразуется в исходный.

Ключ - информация, необходимая для беспрепятственного шифрования и дешифрования текстов.

Криптосистемы разделяются на симметричные и с открытым ключом (ассиметрические).

В симметричных криптосистемах для шифрования и для дешифрования используется один и тот же ключ.

В системах с открытым ключом используются два ключа - открытый и закрытый, которые математически связаны друг с другом. Информация шифруется с помощью открытого ключа, который доступен всем желающим, а расшифровывается с помощью закрытого ключа, известного только получателю сообщения.

Рассмотрим пример криптосистемы с открытым ключом RSA.

Система RSA (Rivest, Shamir, Aldeman) была предложена в 1978 г. И в настоящее время является наиболее распространенной системой шифрования с открытым ключом.

При создании шифров используются различные математические средства. Криптосистема RSA использует теорию сравнений.

Пусть $n = p \cdot q$ — целое число, представимое в виде произведения двух больших простых чисел p, q. Выберем числа e и d из уловия

$$e \cdot d \equiv 1 (mod\ \varphi(n)), \qquad (1)$$

где $\varphi(n) = (p-1)\cdot(q-1)$ — значение функции Эйлера от числа n.

Пусть $k = (n, p, q, e, d)$ — выбранный ключ, состоящий из открытого ключа $k_з = (n, e)$ и секретного ключа $k_p = (n, p, q, d)$.

Пусть M — блок открытого текста и C — соответствующий блок шифрованного текста.

Тогда правила зашифрования и расшифрования определяются формулами:

$$C = E_k(M) = M^e \ (mod\ n); \quad D_k(C) = C^d \ (mod\ n);$$

где $E_k(M)$- множество преобразований зашифрования информации. $D_k(C)$- множество преобразований расшифрования информации.

Криптографические системы с открытым ключом используют так называемые необратимые или односторонние функции, которые обладают следующим свойством: при заданном значении x относительно просто вычислить значение f(x), однако если y=f(x), то нет простого пути для вычисления значения x.

Множество классов необратимых функций и порождает все разнообразие систем с открытым ключом. Однако не всякая необратимая функция годится для использования в реальных информационных системах.

Алгоритмы шифрования с открытым ключом получили широкое распространение в современных информационных системах.

Вообще же все предлагаемые сегодня криптосистемы с открытым ключом опираются на один из следующих типов необратимых преобразований:

- Разложение больших чисел на простые множители;
- Вычисление логарифма в конечном поле;
- Вычисление корней алгебраических уравнений.

Библиографический список:

1. Алферов А.Ю., Зубов А.С. Основы криптографии. – М.: Наука, 2004-423с.
2. Галуев Г.А. Математические основы криптологии: Учебно-методическое пособие. - Таганрог: Изд-во ТРТУ, 2003.-120с.
3. Жельников В. Криптография от папируса до компьютера. – М.: ABF, 1997-336с.
4. Молдовян А. А. и др. Криптография.– СПб.: БХВ-Петербург, 2005-270с.
5. Петров А. А. Компьютерная безопасность. Криптографические методы защиты. – М.: ДМК, 2000-150с.
6. Шнайер Б. Прикладная криптография. – СПб.: БХВ-Петербург, 2002-260с.