(Продолжение. Начало в № 2 (9) за 2005 г.)

Ю. С. Антонов,
кандидат физико-математических наук

Мы рассматривали до сих пор системы симметричной шифровки. В таких системах знание способа шифровки сообщения означает также знание способа его расшифровки. Шифрующий ключ в подобных системах должен передаваться принимающей сообщения стороне со строгим соблюдением секретности. Очевидно, что это мешает массовому применению симметричных криптосистем. С 1978 года широкое применение находят способы несимметричной шифровки. В этих криптосистемах знание способа шифровки текста не помогает в расшифровке криптограммы! Применение однонаправленных функций позволяет легко шифровать текст, но для его расшифровки эффективных вычислительных алгоритмов нет. В качестве примера рассмотрим американскую криптосистему шифрования RSA. В ней в качестве однонаправленной функции применяется операция умножения. Прямая задача – вычисление произведения двух больших простых целых чисел P и Q, то есть нахождение значения $N = P \times Q$, является несложной задачей для компьютера. Для обратной задачи – нахождения множителей P и Q большого целого числа N – до сих пор не найдено эффективного численного алгоритма. Именно поэтому, пользуясь этим алгоритмом, можно свободно давать всем открытый ключ шифровки k_o и число N. Зашифрованные этим ключом тексты расшифровать можете только Вы, так как простые числа P и Q, необходимые для расшифровки, знаете только Вы. Определить эти числа, даже перехватив шифротекст, никто не сможет.

Пусть P = 3, Q = 11, N = 33. Для вычисления закрытого ключа $k_з$ нам понадобится функция Эйлера φ. Тогда

$$\varphi(N) = (P \times Q) = (P - 1) \times (Q - 1) = 20.$$

Открытый ключ и число φ(N) не должны иметь общих множителей. Поэтому в качестве открытого ключа возьмем число 7. Вычислим закрытый ключ из соотношения $k_з \times k_o = 1 \pmod{20}$. Здесь (mod 20) – это остаток от деления на 20. Поэтому $k_з \times k_o = 1 \pmod{20}$ означает, что разделив $k_з \times k_o$ на 20, в остатке получим 1. Число 20 взято не случайно. Это значение функции Эйлера φ от $(P \times Q)$. Подставляя значение открытого ключа, получим: $k_з \times 7 = 1 \pmod{20}$. Ясно, что $k_з = 3$, так как $3 \times 7 = 21 \pmod{20}$. В то же время, $21 \pmod{20} = 21 - 20 = 1$.

Предположим, что нам хотят передать сообщение ВАС. Пусть буквы В, А, С имеют соответственно коды 2, 1, 3. С использованием открытого ключа 7 они будут зашифрованы следующим образом:

$2^7 \pmod{33} = 128 \pmod{33} = 29 \pmod{33}$;

$1^7 \pmod{33} = 1 \pmod{33}$;

$3^7 \pmod{33} = 81 \times 27 = 15 \times 27 = 5 \times 81 = 5 \times 15 = 9 \pmod{33}$.

В итоге мы получаем сообщение: 29, 1, 9. Чтобы расшифровать его, используем закрытый ключ 3:

$29^3 \pmod{33} = (-4)^3 \pmod{33} = (-64) \pmod{33} = 2 \pmod{33} = B$;

$1^3 \pmod{33} = 1 \pmod{33} = A$;

$9^3 \pmod{33} = 81 \times 9 = 15 \times 9 = 135 = 3 \pmod{33} = C$.

Из этого примера видно, что для расшифровки текста надо знать закрытый ключ, но он известен только Вам. Злоумышленнику, чтобы расшифровать текст по перехваченным сообщениям, надо определить простые множители числа N и вычислить для него значение функции Эйлера φ. О трудности этой задачи говорит такой факт. В 1994 году математикам А. Ленстра и М. Манасси удалось найти множители числа, содержащего 129 цифр. Для этого понадобилось 8 месяцев непрерывной работы 1600 компьютеров. Отметим, что криптосистема RSA в настоящее время работает с числами, содержащими 250–300 цифр!

Системы несимметричной шифровки обладают еще одним интересным свойством. Если Вы сообщите всем свой закрытый ключ, а открытый будете держать в тайне, то Ваше зашифрованное сообщение прочтут все обладатели закрытого ключа. В то же время, зашифровать сообщение как Вы, никто не сможет. Этот факт можно использовать для формирования Вашей электронной подписи. Она будет известна всем обладателям закрытого ключа, но никто не сможет подписаться как Вы.

Для защиты от перехвата больших по объему сообщений, кроме цифровой подписи, широко применяется хэширование сообщения. Для этого документ разбивается на блоки. После шифровки первого блока каждая буква зашифрованного первого блока складывается с соответствующей буквой второго блока, например, по модулю 33. Затем результат шифруется, складывается с третьим блоком и так до конца сообщения. Полученное в итоге хэширования окончательное сообщение называется дайджестом исходного сообщения. Понятно, что любые изменения в сообщении, сделанные недобросовестными промежуточными пользователями, изменят и дайджест сообщения. Получатель сообщения, в которое обычно входит электронная подпись отправителя и дата отсылки, вычисляет дайджест сообщения и сравнивает его с полученным дайджестом. Их несовпадение означает некорректность полученного сообщения.

Решение задачи предыдущего номера (№ 2 (11), 2006).

Пронумеруем буквы сообщений и пробелы, передаваемые из пункта А, следующим образом: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12. В пункт Б буквы этих сообщений придут в таком порядке: 2, 4, 6, 8, 10, 12, 1, 3, 5, 7, 9, 11. При использовании шифра замены одинаковые буквы переходят в одинаковые буквы шифротекста, а разные буквы – в разные буквы шифротекста. После передачи сообщений из пункта Б в пункт В символы первоначальных сообщений расположатся в порядке: 4, 8, 12, 3, 7, 11, 2, 6, 10, 1, 5, 9. При этом опять используется шифр замены. Поэтому, одинаковые буквы шифротекста, полученные в пункте Б, перейдут в одинаковые буквы шифротекста, получаемого в пункте В, а разные буквы шифротекста пункта Б – в разные буквы шифротекста пункта В. Восстановим правильный порядок букв в сообщениях из пункта А:

Л П Г С Ж Н Ж О О Б Т –
Е С К Р У П Д С Б Х К Т
Ю У П – О Б Ф Е Б – П –
Л Ж Е С Ж У О П Л У К –
Щ К Х С П Г Б М Ы О Э Ц
Л К Л У Ж Н – Л Г Т И К

Слово КРИПТОГРАФИЯ может быть или вторым, или пятым сообщением, так как только эти сообщения не содержат пробелов. Зашифрованное слово КРИПТОГРАФИЯ должно иметь одинаковые второй и восьмой, а также третий и одиннадцатый символы. Этим признакам удовлетворяет второе сообщение. Перепишем еще раз сообщения, поместив под каждым из них разгаданные буквы:

Л П Г С Ж Н Ж О О Б Т –
* О * Р * * * * * А Я –
Е С К Р У П Д С Б Х К Т
К Р И П Т О Г Р А Ф И Я
Ю У П – О Б Ф Е Б – П –
* Т О – * А * К А – О –
Л Ж Е С Ж У О П Л У К –
* * К Р * Т * * * Т И –
Щ К Х С П Г Б М Ы О Э Ц
* И Ф Р О * А * * * * *
Л К Л У Ж Н – Л Г Т И К
* И * Т * * – * * Я * И

Можно догадаться, что здесь шестая строка должна быть такой: «Э Т О – Н А У К А – О –». Тем самым мы нашли шифры букв Э, Н, У. Теперь можно определить, что вторая строка означает «С О В Р Е М Е Н Н А Я». Продолжая дальше аналогичным образом, разгадываем все сообщение.

Ответ:

С О В Р Е М Е Н Н А Я –
К Р И П Т О Г Р А Ф И Я
Э Т О – Н А У К А – О –
С Е К Р Е Т Н О С Т И –
Ш И Ф Р О В А Л Ь Н Ы Х
С И С Т Е М – С В Я З И

Литература

1. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. – М.: Радио и связь, 1999. – 328 с.

2. Введение в криптографию / Под общей ред. В.В. Ященко. – СПб.: Питер, 2001. – 288 с.

3. JeDaev Alex. Я люблю компьютерную самооборону: Учеб. пособие. – М.: Только для взрослых, 2002. – 432 с.