Федеральное агентство по образованию Российской Федерации

Дальневосточный государственный университет
Институт математики и компьютерных наук

Реферат

Криптоанализ RSA

Выполнил:
студент 246 группы
Соловец Александр

Преподаватель:
Шевченко И.И.

Владивосток
2009

1. Схема шифрования RSA.

Прежде всего вспомним саму схему о.ш и ЭЦП RSA.
1. Выбираются p, q - большие простые числа. Вычисляется произведение $n = pq$.
2. Выбирается число e – такое, что $(e, \varphi(n)) = 1$ (т.е e и $\varphi(n)$ - взаимнопросты), где $\varphi(n)$ – функция Эйлера от n.
3. Из уравнения $ed = 1(mod\ \varphi(n))$ находится число d.

Полученные числа e, n – открытый ключ пользователя, а d – секретный ключ.

Процедура зашифрования: $C = E_{(e,n)}(M) = M^e(modn)$, где -получаемый ш.т. , M - о.т., удовлетворяющий следующему условию: $M^{\varphi(n)} = 1(mod\ n)$.

Процедура расшифрования: $M = D_{(d,n)}(C) = C^d(mod\ n)$.

Генерация цифровой подписи: цифровая подпись $Q = M_d(mod\ n)$.

Проверка цифровой подписи: $Q^e(mod\ n) = M$.

2. Метод безключевого чтения RSA.

Начальные условия. Противнику известны открытый ключ (e, n) и шифротекст .

Задача. Найти исходный текст M.

Противник подбирает число j, для которого выполняется следующее соотношение: $C^{e^j}(mod\ n) = C$. Т.е. противник просто проводит j раз зашифрование на открытом ключе перехваченного шифротекста (это выглядит следующим образом: $(C^e)^e)^e..)^e(mod\ n) = C^{e^j}(mod\ n)$). Найдя такое j, противник вычисляет $C^{e^{j-1}}(mod\ n)$ (т.е. $j-1$ раз повторяет операцию зашифрования) - это значение и есть открытый текст M ! Это следует из того, что $C^{e^j}(mod\ n) = (C^{e^{j-1}}(mod\ n))^e = C$. Т.е некоторое число $C^{e^{j-1}}(mod\ n)$ в степени e дает шифротекст . А что же это, как не открытый текст M?

Пример. $p = 983, q = 563, e = 49, M = 123456$.
$C = M^{49}(mod\ n) = 1603, C^{49^7}(mod\ n) = 85978, C^{49^8}(mod\ n) = 123456, C^{49^9}(mod\ n) = 1603$.

3. Атака на подпись RSA в схеме с нотариусом.

Начальные условия. Имеется электронный нотариус, подписывающий проходящие через него документы. N – некоторый открытый текст, который нотариус не желает подписывать. Противнику известны открытый ключ (e, n) нотариуса.

Задача. Подписать этот текст N.

Противник вырабатывает некое случайное число x, которое взаимнопросто с N и вычисляет $y = x^e(mod\ n)$. Затем получает значение $M = yN$ и передает его на подпись нотариусу. Тот подписывает (ведь это уже не текст N!) $M^d(mod\ n) = S$. Т.е получаем, что $S = M^d(mod\ n) = y^d N^d = (x^e)^d N^d = xN^d$, а значит $N^d = Sx^{-1}(mod\ n)$. Т.е надо просто поделить полученное S на x.

Защита. При подписи добавлять некоторое случайное число в сообщение (например, время). Таким образом получится искажение числа M при подписи.

4. Атака на подпись RSA по выбранному шифротексту.

Начальные условия. Имеется шифротекст C. Противнику известны открытый ключ (e, n) отправителя сообщения.

Задача. Найти исходный текст M.
Противник вырабатывает некое $r : r < n, (r, n) = 1$ и вычисляет $x = r^e (mod\ n)$. Затем о вычисляет $t = r^{-1} (mod\ n)$ и $y = xC (mod\ n)$ и посылает у на подпись отправителю.
Отправитель, ничего не подозревая, подписывает текст $y : w = y^d (mod\ n)$ и отправляет w обратно.
Противник вычисляет $tw (mod\ n) = r^{-1} y^d (mod\ n) =$ (поскольку $r = x^d mod\ n) = x^{-d} x^d C^d (mod\ n) = C^d = M$.
Противник не может сразу послать C на подпись, т.к. отправитель просматривает полученные в результате подписи сообщения и может заметить провокацию.
Атака носит несколько гипотетический характер, но тем не менее позволяет сделать несколько важных выводов:

а) подписывать и шифровать надо разными ключами, либо

б) добавлять случайный вектор при подписи или использовать хэш-функцию.

3. Литература.

1. Т. Корменб, Ч. Лейзерсон, Р. Ривест Алгоритмы: построение и анализ / Пер. с англ. под ред. А. Шеня. – М.: МЦНМО: БИНОМ. Лаборатория знаний, 2004. - 2-е изд., стереотип. – 960 с.

2. http://algolist.manual.ru/defence/attack/rsa.php