SOME PUBLIC-KEY CRYPTO-FUNCTIONS AS INTRACTABLE AS FACTORIZATION

H. C. Williams
Dept. of Computer Science
University of Manitoba
Winnipeg, Manitoba
CANADA R3T 2N2

(Extended Abstract)

1. INTRODUCTION

It is well known that if one can factor the modulus $R = pq$ (p,q distinct large primes) of the RSA cryptosystem [4], then the system can be broken. However, it is not known whether the problem of breaking an RSA cryptosystem is equivalent in difficulty to factoring R. Rabin [3] has given a public-key encryption method which is as difficult to break as it is to factor R, but the decryption process produces four possible candidates for the correct message and only one of these is the correct one. If the actual message being transmitted has little or no internal redundancy (e.g., a cryptographic key) there is no way for the sender to allow the recipient to identify the correct message being transmitted. Also, in [1] Lipton has pointed out some other weaknesses in this scheme when it is used as a cryptosystem. Indeed, Rabin only advocated its use as a signature system.

In [5], Williams described a modification of the RSA technique for which it can be shown that breaking the system is equivalent in difficulty to factoring a special form of R (viz. $R = pq$, where $p \equiv 3 \pmod 8$, $q \equiv 7 \pmod 8$). In this system the decryption procedure yields only one message, the one being transmitted. Also, if one uses a large value of e, Lipton's attacks will fail. The difficulty with this system is the fact that R must be of the above-mentioned special form. In this paper we describe a new method of public-key encryption, which has all of the advantages of that given in [5] but for which R can be a product of two arbitrary primes.

2. SOME PROPERTIES OF THE FUNCTIONS X_n, Y_n.

Instead of raising an integer to a power modulo R, as is done in the RSA case, we raise a number α of the form $W_1 + \sqrt{C}\, W_2$ to a power modulo R. Here W_1, W_2 C are integers. We effect this by means of

G.R. Blakley and D. Chaum (Eds.): Advances in Cryptology - CRYPTO '84, LNCS 196, pp. 66-70, 1985.

the functions X_n and Y_n, defined by

$$X_n(W_1,W_2) = (\alpha^n + \bar{\alpha}^n)/2$$
$$Y_n(W_1,W_2) = W_2(\alpha^n - \bar{\alpha}^n)/(\alpha - \bar{\alpha}).$$

Here $\bar{\alpha} = W_1 - \sqrt{C}\, W_2$ and we easily see that

$$\alpha^n = X_n(W_1,W_2) + \sqrt{C}\, Y_n(W_1,W_2).$$

Both functions X_n and Y_n can be computed modulo R in $O(\log n)$ multiplication and division operations. (See, for example, Lehmer [2]).

We require the following

Theorem. Suppose p and q are odd primes and

i) $W_1^2 - C\, W_2^2 \equiv 1 \pmod R$;

ii) The Legendre symbols $\epsilon_p = (C/p) \equiv -p \pmod 4$ and $\epsilon_q = (C/q) \equiv -q \pmod 4$;

iii) $\gcd(CW_2, R) = 1$;

iv) The Jacobi symbol $(2(W_1 + 1)/R) = 1$;

v) $ed \equiv (w + 1)/2 \pmod w$, where

$$w = (p - \epsilon_p)(q - \epsilon_q)/4. \tag{1}$$

Then we must have

$$X_{2ed}(W_1,W_2) \equiv sW_1$$
$$Y_{2ed}(W_1,W_2) \equiv sW_2 \pmod R,$$

where $|s| = 1$. □

3. ENCRYPTION AND DECRYPTION.

To produce his encryption key a designer of our cryptosystem selects two large primes p and q and forms their product R. He then selects, by trial, some integer C such that

$$(C/p) \equiv -p, \quad (C/q) \equiv -q \pmod 4.$$

Again, by trial, he finds some integer A such that the Jacobi symbol

$$(A^2 - C/R) = -1.$$

Finally, for a randomly selected e such that $\gcd(e,w) = 1$ (w given

by (1)), he solves

$$ed \equiv (w + 1)/2 \pmod{w}$$

for d.

The public encryption key is now $\{R,e,C,A\}$ and the secret decryption key is d. Since C and A are usually small, the encryption key does not require much more storage space than that required by the RSA scheme.

Let M be any message $(0 < M < R)$ to be encrypted. We put $b_1 = 0$ when the Jacobi symbol $(M^2 - C/R) = 1$ and we put $b_1 = 1$ when $(M^2 - C/R) = -1$. Define

$$\gamma = \begin{cases} M + \sqrt{C} & \text{when } b_1 = 0 \\ (M + \sqrt{C})(A + \sqrt{C}) & \text{when } b_1 = 1. \end{cases}$$

We have $(\gamma\bar{\gamma}/R) = 1$.
Define T(M) and S(M) by

$$\alpha = \gamma/\bar{\gamma} \equiv T(M) + S(M)\sqrt{C} \pmod{R}.$$

(We say that $(U + V\sqrt{C})/W \equiv T + S\sqrt{C} \pmod{R}$ when $UW^{-1} \equiv T$ and $VW^{-1} \equiv S \pmod{R}$). Note that

$$1 = \alpha\bar{\alpha} \equiv T(M)^2 - CS(M)^2.$$

Further,

$$2(T(M) + 1) \equiv (\gamma + \bar{\gamma})^2(\gamma\bar{\gamma})^{-1} \pmod{R};$$

thus

$$(2(T(M) + 1)/R) = 1.$$

If we put $b_2 \equiv T(M) \pmod 2$ $(b_2 = 0,1)$, we can encrypt M by computing

$$E(M) \equiv X_e(T(M),S(M))\{Y_e(T(M),S(M))\}^{-1} \pmod{R},$$

where $0 < E(M) < R$.

If E(M), along with b_1 and b_2, is sent to the designer of the cryptosystem, then he can compute

$$U \equiv X_{2e}(T(M),S(M)) \equiv (K^2 + C)(K^2 - C)^{-1}$$
$$V \equiv Y_{2e}(T(M),S(M)) \equiv 2K(K^2 - C)^{-1} \pmod{R},$$

where $K = E(M)$. Only he can now determine

$$X_d(U,V) \equiv X_{2ed}(T(M),S(M))$$

$$Y_d(U,V) \equiv Y_{2ed}(T(M),S(M)) \pmod{R}.$$

By the theorem we know that

$$X_d(U,V) \equiv sT(M),\ Y_d(U,V) \equiv sS(M) \pmod{R},$$

where $|s| = 1$. With the value of b_2, it is easy to find s and with b_1, it is easy to determine M from knowledge of both $T(M)$ and $S(M)$.

4. SECURITY.

Suppose that P is some algorithm which decrypts $1/k$ of all ciphertexts produced by our cryptosystem. Find some Z such that

$$(Z^2 - C/R) = -1$$

and

$$\gcd(Z,R) = 1.$$

Compute

$$K \equiv X_e(T,S)Y_e(T,S)^{-1} \pmod{R},$$

where

$$T + S\sqrt{C} \equiv (Z + \sqrt{C})/(Z - \sqrt{C}) \pmod{R}.$$

With probability $1/k$, P will determine some M such that $P(M) = K$. Now for N one of M or $C^{-1}M \pmod{R}$, we have

$$(N^2 - C/R) = 1$$

and

$$Z(N^2 + C) \equiv N(Z^2 + C) \pmod{R};$$

hence, $\gcd(N - Z,R) = p$ or q and R can be factored. Thus, anyone who can decrypt messages sent on this system can factor R.

We must emphasize, however, that since the method of proof utilized here is constructive, this system is susceptible to a known ciphertext attack. Thus, it must be used with certain protocols. Lipton's types of attack, when applied to this scheme, will also fail when e is large; indeed, even if one of the e's is 1, his first attack will fail.

This scheme can also be used to produce signatures, but in this application e must not be 1.

The full details of the work summarized here will appear in a forthcoming issue of Cryptologia.

REFERENCES

[1] R. A. Demillo et al. "On the Safety of Cryptosystems," Applied Cryptology, Cryptographic Protocols and Computer Security Models, AMS Short Course Lecture Notes, Vol. 29, Providence, 1983.

[2] D. H. Lehmer, Computer technology applied to the theory of numbers, Studies in Number Theory, MAA Studies in Mathematics Vol. 6, 1969, pp. 117-151.

[3] M. O. Rabin, "Digitized signatures and public-key functions as intractable as factorization," M.I.T. Lab. for Computer Science, Tech. Rep. LCS/TR212, 1979.

[4] R. L. Rivest, A. Shamir, and L. Adelman, "A method for obtaining digital signatures and public-key cryptosystems," Comm. ACM, 21 (1978), 120-126.

[5] H. C. Williams, "A modification of the RSA public-key encryption procedure," IEEE Transactions on Information Theory, IT-26 (1980), 726-729.