Rabin cryptosystem

The **Rabin cryptosystem** is an asymmetric cryptographic technique, whose security, like that of RSA, is related to the difficulty of factorization. However the Rabin cryptosystem has the advantage that the problem on which it relies has been proven to be as hard as integer factorization, which is not currently known to be true of the RSA problem. It has the disadvantage that each output of the Rabin function can be generated by any of four possible inputs; if each output is a ciphertext, extra complexity is required on decryption to identify which of the four possible inputs was the true plaintext.

Contents

History

The process was published in January 1979 by Michael O. Rabin. The Rabin cryptosystem was the first asymmetric cryptosystem where recovering the entire plaintext from the ciphertext could be proven to be as hard as factoring.

Algorithm

Key generation

As with all asymmetric cryptosystems, the Rabin system uses both a public and a private key. The public key is necessary for later encryption and can be published, while the private key must be possessed only by the recipient of the message.

The precise key-generation process follows:

- Choose two large distinct primes p and q. One may choose $p \equiv q \equiv 3 \bmod 4$ to simplify the computation of square roots modulo p and q (see below). But the scheme works with any primes.
- Let $n = p \cdot q$. Then n is the public key. The primes p and q are the private key.

To encrypt a message only the public key n is needed. To decrypt a ciphertext the factors p and q of n are necessary.

As a (non-real-world) example, if $p = 7$ and $q = 11$, then $n = 77$. The public key, 77, would be released, and the message encoded using this key. And, in order to decode the message, the private keys, 7 and 11, would have to be known (of course, this would be a poor choice of keys, as the factorization of 77 is trivial; in reality much larger numbers would be used).

Encryption

For the encryption, only the public key *n* is used, thus producing a ciphertext out of the plaintext. The process follows:

Let $P = \{0, \ldots, n-1\}$ be the plaintext space (consisting of numbers) and $m \in P$ be the plaintext. Now the ciphertext c is determined by

$$c = m^2 \bmod n.$$

That is, *c* is the quadratic remainder of the square of the plaintext, modulo the key-number *n*.

In our simple example, $P = \{0, \ldots, 76\}$ is our plaintext space. We will take $m = 20$ as our plaintext. The ciphertext is thus $c = m^2 \bmod n = 400 \bmod 77 = 15$.

For exactly four different values of *m*, the ciphertext 15 is produced, i.e. for $m \in \{13, 20, 57, 64\}$. This is true for most ciphertexts produced by the Rabin algorithm, i.e. it is a four-to-one function.

Decryption

To efficiently decode the ciphertext, the private keys *p* and *q* are necessary. The process follows:

If *c* and *n* are known, the plaintext is then $m \in \{0, \ldots, n-1\}$ with $m^2 \equiv c \bmod n$. For a composite *n* (that is, like the Rabin algorithm's $n = p \cdot q$) there is no efficient method known for the finding of *m*. If, however n is prime (or *p* and *q* are, as in the Rabin algorithm), the Chinese remainder theorem can be applied to solve for *m*.

Thus the square roots

$$m_p = \sqrt{c} \bmod p$$

and

$$m_q = \sqrt{c} \bmod q$$

must be calculated (see section below).

In our example we get and $m_q = 9$.

By applying the extended Euclidean algorithm, we wish to find y_p and y_q such that $y_p \cdot p + y_q \cdot q = 1$. In our example, we have $y_p = -3$ and $y_q = 2$.

Now, by invocation of the Chinese remainder theorem, the four square roots $+r$, $-r$, $+s$ and $-s$ of $c + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$ are calculated ($\mathbb{Z}/n\mathbb{Z}$ here stands for the ring of congruence classes modulo *n*). The four square roots are in the set $\{0, \ldots, n-1\}$:

$$\begin{aligned} r &= (y_p \cdot p \cdot m_q + y_q \cdot q \cdot m_p) \bmod n \\ -r &= n - r \\ s &= (y_p \cdot p \cdot m_q - y_q \cdot q \cdot m_p) \bmod n \\ -s &= n - s \end{aligned}$$

One of these square roots is the original plaintext *m*. In our example, .

Finding the factorization of n is possible, as Rabin pointed out in his paper, if *both*, and can be computed, as is either or (where means greatest common divisor). Since the greatest common divisor can be calculated efficiently, the factorization of n can be found efficiently if and are known. In our example (picking and as and):

Computing square roots

The decryption requires to compute square roots of the ciphertext c modulo the primes p and q. Choosing $p \equiv q \equiv 3 \bmod 4$ allows to compute square roots more easily by

and

.

We can show that this method works for p as follows. First implies that $(p+1)/4$ is an integer. The assumption is trivial for $c \equiv 0 \bmod p$. Thus we may assume that p does not divide c. Then

where is a Legendre symbol.

From follows that . Thus c is a quadratic residue modulo p. Hence and therefore

The relation is not a requirement because square roots modulo other primes can be computed too. E.g., Rabin proposes to find the square roots modulo primes by using a special case of Berlekamp's algorithm.

Evaluation of the algorithm

Effectiveness

Decoding produces three false results in addition to the correct one, so that the correct result must be guessed. This is the major disadvantage of the Rabin cryptosystem and one of the factors which have prevented it from finding widespread practical use.

If the plaintext is intended to represent a text message, guessing is not difficult; however, if the plaintext is intended to represent a numerical value, this issue becomes a problem that must be resolved by some kind of disambiguation scheme. It is possible to choose plaintexts with special structures, or to add padding, to eliminate this problem. A way of removing the ambiguity of inversion was suggested by Blum and Williams: the two primes used are restricted to primes congruent to 3 modulo 4 and the domain of the squaring is restricted to the set of quadratic residues. These restrictions make the squaring function into a trapdoor permutation, eliminating the ambiguity.[1]

Efficiency

For encryption, a square modulo *n* must be calculated. This is more efficient than RSA, which requires the calculation of at least a cube.

For decryption, the Chinese remainder theorem is applied, along with two modular exponentiations. Here the efficiency is comparable to RSA.

Disambiguation introduces additional computational costs, and is what has prevented the Rabin cryptosystem from finding widespread practical use.

Security

The great advantage of the Rabin cryptosystem is that a random plaintext can be recovered entirely from the ciphertext only if the codebreaker is capable of efficiently factoring the public key *n*. Note that this is a very weak level of security. Extensions of the Rabin cryptosystem achieve stronger notions of security

It has been proven that decoding the Rabin cryptosystem is equivalent to the integer factorization problem, something that has not been proven for RSA. Thus the Rabin system is 'more secure' in this sense than is RSA, and will remain so until a general solution fo the factorization problem is discovered, or until the RSA problem is discovered to be equivalent to factorization. (This assumes that the plaintext was not created with a specific structure to ease decoding.)

Since the solution to the factorization problem is being sought on many different fronts, any solution (outside classified research organizations such as NSA) would rapidly become available to the whole scientific community. However, a solution has been long in coming, and the factorization problem has been, thus far, practically insoluble. Without such an advance, an attacker would have no chance today of breaking the encryption of random messages.

However, this cryptosystem does not provide indistinguishability against chosen plaintext attacks since the process of encryption is deterministic. An adversary, given a ciphertext and a candidate message, can easily determine whether or not the ciphertext encodes the candidate message (by simply checking whether encrypting the candidate message yields the given ciphertext).

Furthermore, it has been proven an active attacker can break the system using a chosen ciphertext attack (even when challenge messages are chosen uniformly at random from the message space). By adding redundancies, for example, the repetition of the last 64 bits, the system can be made to produce a single root. This thwarts this specific chosen-ciphertext attack, since the decoding algorithm then only produces the root that the attacker already knows. If this technique is applied, the proof of the equivalence with the factorization problem fails, so it is uncertain as of 2004 if this variant is secure. The Handbook of Applied Cryptography by Menezes, Oorschot and Vanstone considers this equivalence probable, however, as long as the finding of the roots remains a two-part process (1. roots and and 2. application of the Chinese remainder theorem).

Since in the encoding process, only the modulo remainders of perfect squares are used (in our example with $n = 77$, this is only 23 of the 76 possible values), other attacks on the process are possible.

See also

- Topics in cryptography
- Blum Blum Shub
- Shanks–Tonelli algorithm
- Schmidt–Samoa cryptosystem
- Blum–Goldwasser cryptosystem

Notes

1. Shafi Goldwasser and Mihir Bellare "Lecture Notes on Cryptography" (http://cseweb.ucsd.edu/~mihir/papers/gb.html) Summer course on cryptography MIT, 1996-2001

References

- Buchmann, Johannes. *Einführung in die Kryptographie* Second Edition. Berlin: Springer, 2001. ISBN 3-540-41283-2
- Menezes, Alfred; van Oorschot, Paul C.; and Vanstone, Scott A. *Handbook of Applied Cryptography* CRC Press, October 1996. ISBN 0-8493-8523-7
- Rabin, Michael. *Digitalized Signatures and Public-Key Functions as Intractable as Factorization* (in PDF). MIT Laboratory for Computer Science, January 1979.
- Scott Lindhurst, An analysis of Shank's algorithm for computing square roots in finite fields. in R Gupta and K S Williams, Proc 5th Conf Can Nr Theo Assoc, 1999, vol 19 CRM Proc & Lec Notes, AMS, Aug 1999.
- R Kumanduri and C Romero, Number Theory w/ Computer Applications, Alg 9.2.9, Prentice Hall, 1997. A probabilistic for square root of a quadratic residue modulo a prime.

External links

- Menezes, Oorschot, Vanstone, Scott: *Handbook of Applied Cryptography* (free PDF downloads), see Chapter 8