WIKIPEDIA

Coppersmith's attack

Coppersmith's attack describes a class of cryptographic attacks on the public-key cryptosystem RSA based on the Coppersmith method. Particular applications of the Coppersmith method for attacking RSA include cases when the public exponent e is small or when partial knowledge of a prime factor of the secret key is available.

Contents

RSA basics

The public key in the RSA system is a tuple of integers (N, e), where N is the product of two primes p and q. The secret key is given by an integer d satisfying $ed \equiv 1 \pmod{(p-1)(q-1)}$; equivalently, the secret key may be given by $d_p \equiv d \pmod{p-1}$ and $d_q \equiv d \pmod{q-1}$ if the Chinese remainder theorem is used to improve the speed of decryption, see CRT-RSA. Encryption of a message M produces the ciphertext $C \equiv M^e \pmod N$, which can be decrypted using d by computing $C^d \equiv M \pmod N$.

Low public exponent attack

In order to reduce encryption or signature verification time, it is useful to use a small public exponent (e). In practice, common choices for e are 3, 17 and 65537 $(2^{16}+1)$. These values for e are Fermat primes, sometimes referred to as F_0, F_2 and F_4 respectively $(F_x = 2^{2^x}+1)$. They are chosen because they make the modular exponentiation operation faster. Also, having chosen such e, it is simpler to test whether $\gcd(e, p-1) = 1$ and $\gcd(e, q-1) = 1$ while generating and testing the primes in step 1 of the key generation. Values of p or q that fail this test can be rejected there and then. (Even better: if e is prime and greater than 2, then the test $p \bmod e \neq 1$ can replace the more expensive test $\gcd(p-1, e) = 1$.)

If the public exponent is small and the plaintext m is very short, then the RSA function may be easy to invert, which makes certain attacks possible. Padding schemes ensure that messages have full lengths, but additionally choosing public exponent $e = 2^{16}+1$ is recommended. When this value is used, signature verification requires 17 multiplications, as opposed to about 25 when a random e of similar size is used. Unlike low private exponent (see Wiener's attack), attacks that apply when a small e is used are far from a total break, which would recover the secret key d. The most powerful attacks on low public exponent RSA are based on the following theorem, which is due to Don Coppersmith.

Coppersmith method

Theorem 1 (Coppersmith)[1]

Let N be an integer and $f \in \mathbb{Z}[x]$ be a monic polynomial of degree d over the integers. Set $X = N^{\frac{1}{d}-\epsilon}$ for $\frac{1}{d} > \epsilon > 0$. Then, given $\langle N, f\rangle$, attacker (Eve) can efficiently find all integers $x_0 < X$ satisfying $f(x_0) \equiv 0 \pmod N$. The running time is dominated by the time it takes to run the LLL algorithm on a lattice of dimension $\mathrm{O}(w)$ with $w = \min\left\{\frac{1}{\epsilon}, \log_2 N\right\}$.

This theorem states the existence of an algorithm that can efficiently find all roots of f modulo N that are smaller than $X = N^{\frac{1}{d}}$. As X gets smaller, the algorithm's runtime decreases. This theorem's strength is the ability to find all small roots of polynomials modulo a composite N.

Håstad's broadcast attack

The simplest form of Håstad's attack[2] is presented to ease understanding. The general case uses the Coppersmith method.

Suppose one sender sends the same message M in encrypted form to a number of people $P_1; P_2; \ldots; P_k$, each using the same small public exponent e, say $e = 3$, and different moduli $\langle N_i, e\rangle$. A simple argument shows that as soon as $k \geq 3$ ciphertexts are known, the message M is no longer secure: Suppose Eve intercepts C_1, C_2, and C_3, where $C_i \equiv M^3 \pmod{N_i}$. We may assume $\gcd(N_i, N_j) = 1$ for all i, j (otherwise, it is possible to compute a factor of one of the numbers N_i by computing $\gcd(N_i, N_j)$.) By the Chinese remainder theorem, she may compute $C \in \mathbb{Z}^*_{N_1N_2N_3}$ such that $C \equiv C_i \pmod{N_i}$. Then $C \equiv M^3 \pmod{N_1N_2N_3}$; however, since $M < N_i$ for all i, we have $M^3 < N_1N_2N_3$. Thus $C = M^3$ holds over the integers, and Eve can compute the cube root of C to obtain M.

For larger values of e, more ciphertexts are needed, particularly, e ciphertexts are sufficient.

Generalizations

Håstad also showed that applying a linear padding to M prior to encryption does not protect against this attack. Assume the attacker learns that $C_i = f_i(M)^e$ for $1 \leq i \leq k$ and some linear function f_i, i.e., Bob applies a pad to the message M prior to encrypting it so that the recipients receive slightly different messages. For instance, if M is m bits long, Bob might encrypt $M_i = i2^m + M$ and send this to the i-th recipient.

If a large enough group of people is involved, the attacker can recover the plaintext M_i from all the ciphertext with similar methods. In more generality, Håstad proved that a system of univariate equations modulo relatively prime composites, such as applying any fixed polynomial $g_i(M) \equiv 0 \pmod{N_i}$, could be solved if sufficiently many equations are provided. This attack suggests that randomized padding should be used in RSA encryption.

Theorem 2 (Håstad)

Suppose $N_1, \ldots, N_k$ are relatively prime integers and set $N_{\min} = \min_i\{N_i\}$. Let $g_i(x) \in \mathbb{Z}/N_i[x]$ be k polynomials of maximum degree q. Suppose there exists a unique $M < N_{\min}$ satisfying $g_i(M) \equiv 0 \pmod{N_i}$ for all $i \in \{1, \ldots, k\}$. Furthermore, suppose $k > q$. There is an efficient algorithm that, given $\langle N_i, g_i(x)\rangle$ for all i, computes M.

Proof

Since the N_i are relatively prime the Chinese remainder theorem might be used to compute coefficients T_i satisfying $T_i \equiv 1 \pmod{N_i}$ and $T_i \equiv 0 \pmod{N_j}$ for all $i \neq j$. Setting $g(x) = \sum T_i \cdot g_i(x)$, we know that $g(M) \equiv 0 \pmod{\prod N_i}$. Since the T_i are nonzero, we have that $g(x)$ is also nonzero. The degree of $g(x)$ is at most q. By Coppersmith's theorem, we may compute all integer roots x_0 satisfying $g(x_0) \equiv 0 \pmod{\prod N_i}$ and $|x_0| < \left(\prod N_i\right)^{\frac{1}{q}}$. However, we know that $M < N_{\min} < \left(\prod N_i\right)^{\frac{1}{k}} < \left(\prod N_i\right)^{\frac{1}{q}}$, so M is among the roots found by Coppersmith's theorem.

This theorem can be applied to the problem of broadcast RSA in the following manner: Suppose the i-th plaintext is padded with a polynomial $f_i(x)$, so that $g_i = \left(f_i(x)\right)^{e_i} - C_i \bmod N_i$. Then $g_i(M) \equiv 0 \bmod N_i$ is true, and Coppersmith's method can be used. The attack succeeds once $k > \max_i(e_i \cdot \deg f_i)$, where k is the number of messages. The original result used Håstad's variant instead of the full Coppersmith method. As a result, it required $k = O(q^2)$ messages, where $q = \max_i(e_i \cdot \deg f_i)$.[2]

Franklin–Reiter related-message attack

Franklin and Reiter identified an attack against RSA when multiple related messages are encrypted: If two messages differ only by a known fixed difference between the two messages and are RSA-encrypted under the same RSA modulus N, then it is possible to recover both of them. The attack was originally described with public exponent $e = 3$, but it works more generally (with increasing cost as e grows).

Let $\langle N; e_i\rangle$ be Alice's public key. Suppose $M_1; M_2 \in \mathbb{Z}_N$ are two distinct messages satisfying $M_1 \equiv f(M_2) \pmod N$ for some publicly known polynomial $f \in \mathbb{Z}_N[x]$. To send M_1 and M_2 to Alice, Bob may naively encrypt the messages and transmit the resulting ciphertexts $C_1; C_2$. Eve can easily recover $M_1; M_2$, given $C_1; C_2$, by using the following theorem:

Theorem 3 (Franklin–Reiter)[1]

Let $\langle N, e\rangle$ be an RSA public key. Let $M_1 \neq M_2 \in \mathbb{Z}^*_N$ satisfy $M_1 \equiv f(M_2) \pmod N$ for some linear polynomial $f = ax + b \in \mathbb{Z}_N[x]$ with $b \neq 0$. Then, given $\langle N, e, C_1, C_2, f\rangle$, attacker (Eve) can recover M_1, M_2 in time quadratic in $e \cdot \log N$.

Proof

Since $C_1 \equiv M_1^e \pmod N$, we know that M_2 is a root of the polynomial $g_1(x) = f(x)^e - C_1 \in \mathbb{Z}_N[x]$. Similarly, M_2 is a root of $g_2(x) = x^e - C_2 \in \mathbb{Z}_N[x]$. Hence, the linear factor $x - M_2$ divides both polynomials. Therefore, Eve may calculate the greatest common divisor $\gcd(g_1, g_2)$ of g_1 and g_2, and if the $\gcd$ turns out to be linear, M_2 is found. The $\gcd$ can be computed in quadratic time in e and $\log N$ using the Euclidean algorithm.

Coppersmith's short-pad attack

Like Håstad's and Franklin–Reiter's attacks, this attack exploits a weakness of RSA with public exponent $e = 3$. Coppersmith showed that if randomized padding suggested by Håstad is used improperly, then RSA encryption is not secure.

Suppose Bob sends a message M to Alice using a small random padding before encrypting it. An attacker, Eve, intercepts the ciphertext and prevents it from reaching its destination. Bob decides to resend M to Alice because Alice did not respond to his message. He randomly pads M again and transmits the resulting ciphertext. Eve now has two ciphertexts corresponding to two encryptions of the same message using two different random pads.

Even though Eve does not know the random pad being used, she still can recover the message M by using the following theorem, if the random padding is too short.

Theorem 4 (Coppersmith)

Let $\langle N, e\rangle$ be a public RSA key, where N is n bits long. Set $m = \left\lfloor \frac{n}{e^2} \right\rfloor$. Let $M \in \mathbb{Z}^*_N$ be a message of length at most $n - m$ bits. Define $M_1 = 2^m M + r_1$ and $M_2 = 2^m M + r_2$, where r_1 and r_2 are distinct integers with $0 \leq r_1, r_2 < 2^m$. If Eve is given $\langle N, e\rangle$ and the encryptions C_1, C_2 of M_1, M_2 (but is not given r_1 or r_2), she can efficiently recover M.

Proof[1]

Define $g_1(x, y) = x^e - C_1$ and $g_2(x, y) = (x+y)^e - C_2$. We know that when $y = r_2 - r_1$, these polynomials have $x = M_1$ as a common root. In other words, $\Delta = r_2 - r_1$ is a root of the resultant $h(y) = \mathrm{res}_x(g_1, g_2) \in \mathbb{Z}_N[y]$. Furthermore, $|\Delta| < 2^m < N^{\frac{1}{e^2}}$. Hence, Δ is a small root of h modulo N, and Eve can efficiently find it using the Coppersmith method. Once Δ is known, the Franklin–Reiter attack can be used to recover M_2 and consequently M.

See also

- ROCA attack

References

1. D. Boneh, Twenty years of attacks on the RSA cryptosystem (http://crypto.stanford.edu/~dabo/pubs/papers/RSA-survey.pdf).
2. Glenn Durfee, Cryptanalysis of RSA Using Algebraic and Lattice Methods (http://theory.stanford.edu/~gdurf/durfee-thesis-phd.pdf).