LECTURE 10, FEB 15, 2011,RSA

Chinese remainder theorem. We have shown that the $x_0 = a_1 m_2 y_1 + a_2 m_1 y_2$ is a solution. It is also clear that the integers of the form $x_0 + \ell m_1 m_2$ are also solutions to the equations. It remains to show that all the solutions can be expressed in this way.

Assume x is another solution to the problem, and we have

$$x \equiv x_0 \mod m_1$$
$$x \equiv x_0 \mod m_2$$

By definitions, there exists integer p and q such that $x - x_0 = pm_1 = qm_2$. This suggests that $m_1 | qm_2$. Since $\gcd(m_1, m_2) = 1$, we have $m_1 | q$ and we can rewrite q as $q' m_1$ for some integer q'.

Therefore, we have $x - x_0 = q' m_1 m_2$. □

We can extend the results to the case with more than two equations:

$$x \equiv a_1 \mod m_1$$
$$x \equiv a_2 \mod m_2$$
$$\cdots$$
$$x \equiv a_k \mod m_k,$$

Assume $m_1, m_2, \dots, m_k$ are pairwise relative prime, then we first solve

$$M_1 y_1 \equiv 1 \mod m_1$$
$$M_2 y_2 \equiv 1 \mod m_2$$
$$\cdots$$
$$M_k y_k \equiv 1 \mod m_k,$$

where

$$M_j = \frac{m_1 m_2 \cdots m_k}{m_j}$$

Then one solution to the equation is given by

$$x_0 = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots a_k M_k y_k,$$

and all other solutions are of the form $x_0 + \ell m_1 m_2 \cdots m_k$, where ℓ is some integer.

The Chinese remainder theorem can be used to represent large integers. We select moduli such that they are pairwise relative prime. Then for any integer a, we represent it as a tuple

$$(a \mod m_1, a \mod m_2, \dots, a \mod m_k)$$

Then, we can perform arithmetic operations on the components. For instance, let the moduli be 99, 98, 97, and 95. Then $123684 = (33, 8, 9, 89)$ and $413456 = (32, 92, 42, 16)$.

$$(33, 8, 9, 89) + (32, 92, 42, 16) = (65, 2, 51, 10)$$

Solving

$$\begin{aligned} x &\equiv 65 \mod 99 \\ x &\equiv 2 \mod 98 \\ x &\equiv 51 \mod 97 \\ x &\equiv 10 \mod 95 \end{aligned}$$

recovers the correct solution 537140.

Now we consider cryptography. The sender (Alice) wants to encrypt a message such that the intended receiver (Bob) is able to decipher it.

Traditionally, Alice and Bob agree on a secret code ahead of the time, and use it to both encrypt and decipher the message. For instance, they may agree to shift the alphabeta by some fixed number of positions. The weakness is the secret code. It may be stolen or cracked.

On the other hand, we have what is called a public key cryptography. In this setting, each people has a public key and a private key, and they transmit the message in this way.

(1) Bob gets Alice's public key P_A.
(2) Bob encrypts his message $c = P_A(M)$.
(3) Bob sends c to Alice.
(4) Alice deciphers the code using her private key $M = S_A(c)$.

This process requires: (a) the public key should be easy to compute, meaning it doesn't take too much time to encrypt a message; (b) the public key should have an inverse so that the message can be deciphered; (c) the inverse function should be only easy to compute for the owner.

Specifically,

(1) Choose two large primes p and q and let $n = pq$.
(2) Choose $e \neq 1$ relative prime to $(p-1)(q-1)$ and let d be its multiplicative inverse modulo $(p-1)(q-1)$.
(3) The public keys are n and e, and the private key is d.

$$\begin{aligned} f &= x^e \mod n \\ f^{-1} &= x^d \mod n \end{aligned}$$

Correctness of RSA. We need to show that

$$(M^e)^d \equiv M \mod n.$$

Since e and d are multiplicative inverses modulo $(p-1)(q-1)$,

$$ed = 1 + k(p-1)(q-1),$$

for some integer k. Then, if M is not divisible by p, we have

$$\begin{aligned} M^{ed} &\equiv M^{1+k(p-1)(q-1)} \mod p \\ &\equiv M(M^{p-1})^{k(q-1)} \mod p \\ &\equiv M 1^{k(q-1)} \mod p \\ &\equiv M \end{aligned}$$

Also, $M^{ed} \equiv M \mod p$ if M is divisible by p. Thus,

$$M^{ed} \equiv M \mod p, \quad \forall M.$$

Similarly, we have

$$M^{ed} \equiv M \mod q, \quad \forall M.$$

By Chinese remainder theorem, we have

$$M^{ed} \equiv M \mod (pq), \quad \forall M.$$

□

Attacks against plain RSA: if an attacker wants to know the decryption of a ciphertext $c = m^e \mod n$, he may ask the holder of the private key to decipher an unsuspicious-looking ciphertext $c' = cr^e \mod n$ for some value r chosen by the attacker. Because c' is the encryption of $mr \mod n$, hence if the attacker knows $mr \mod n$, he can then multiplying with the multiplicative inverse of r to get m.