Scribe: Cryptography and Network Security (Week-10 Class-3)

Smayan Das

06-Nov-2020

1 Introduction

The Chinese remainder theorem is a theorem which gives a unique solution to simultaneous linear congruences with coprime moduli.
This lecture focuses on understanding the Chinese Remainder Theorem and its applications in Cryptography.

2 The Chinese Remainder Theorem

Theorem *Every system of linear congruences $x \equiv a_1 \pmod{m_1}, \ldots, x \equiv a_n \pmod{m_n}$, in which the moduli are relatively prime in pairs, is solvable, and the solution is unique modulo the product of the moduli.*

Proof: The theorem is trivially true if there is only one congruence in the system. Suppose that it is true for every system containing fewer than n congruences, and consider the system $x \equiv a_i \pmod{m_i}$, $i = 1, \ldots, n$, in which $(m_i, m_j) = 1$ for $1 \leq i \leq j \leq n$. Then by the induction hypothesis we can solve the last $n-1$ of the congruences simultaneously, and obtain in their place a single congruence with modulus $m_2 \cdots m_n$. Put $m_2 \cdots m_n = M$. Then the system of n congruences is equivalent to the simple system

$$x \equiv a_1 \pmod{m_1}, \quad x \equiv A \pmod{M},$$

for suitable A. Repeating the reasoning used above, we find

$$x = a_1 + m_1 y,$$
$$a_1 + m_1 y \equiv A \pmod{M},$$
$$m_1 y \equiv A - a_1 \pmod{M},$$

and since $(m_1, M) = 1$, this last congruence has a unique solution $\pmod{M}$ (proved later). If the solution is $y \equiv A' \pmod{M}$, then we have

$$y = A' + Mz,$$
$$x = a_1 + m_1(A' + Mz) = (a_1 + m_1 C') + m_1 M z,$$

and so x is unique modulo $m_1 M = m_1 \cdots m_n$.

2.1 Uniqueness

The uniqueness part of CRT states that there is at most 1 solution, and the existence part of CRT states that there is at least 1 solution. Here, we will prove the uniqueness part, which is quite straightforward.

Proof: Let X_1 and X_2 be any two solutions to the above system of congruences. This implies that:

$$X_1 \equiv X_2 \equiv a_1 \pmod{m_1}$$

Thus m_1 divides $X_1 - X_2$ and by a similar reasoning m_i divides $X_1 - X_2$ for all $1 \leq i \leq n$. Let d denote the LCM of $m_1, m_2, ..., m_n$ then d divides $X_1 - X_2$. Now as $m_1, m_2, ..., m_n$ are all relatively prime so,

$$d = m_1 m_2 m_3 ... m_n$$

Thus, $m_1 m_2 m_3 ... m_n$ divides $X_1 - X_2$ which means

$$X_1 \equiv X_2 \pmod{m_1 m_2 m_3 ... m_n}$$

This clearly means that $X_1 = X_2$ and hence the system of equations has at most 1 solution modulo $m_1 m_2 m_3 ... m_n$.

2.2 General Construction

The following is a general construction to find a solution to a system of congruences using the Chinese Remainder Theorem:

- Compute $M = m_1 m_2 m_3 ... m_n$
- For each i = 1,2,3....n, compute:

  $$M_i = \frac{M}{m_1}$$

- Now for each i = 1,2,3....n, compute

  $$y_i = M_i^{-1} \pmod{m_i}$$

- Finally compute

  $$x = \sum_{i=1}^{n} a_i M_i y_i$$

  which gives a solution to the syste of congruences and x is a unique solution modulo M.

3 Using Chinese Remainder Theorem with RSA Algorithm

The Chinese Remainder Theorem (CRT) can be used to speed up the calculations for the RSA algorithm.

The idea behind the CRT optimization is that if we know the factorization of the modulus M (which we may if we have the private key), then we can split up the message P into two halves y_1 and y_2 (one modulo p, and one modulo q), compute each modulo separately, and then recombine them. Thus, here, the exponents are reduced modulo p1 and q1(which speeds things up) using the fact that p and q are prime and then applying Fermat's little theorem as follows:

$$y_1 = (P^d \bmod M) \bmod p = ((P \bmod p)^{d \bmod p-1}) \bmod p$$

$$y_2 = (P^d \bmod M) \bmod q = ((P \bmod q)^{d \bmod q-1}) \bmod q$$

Then we recombine them that is we find a number n such that

$$n \equiv (P^d \bmod M) \pmod p$$

$$n \equiv (P^d \bmod M) \pmod q$$

Now, because of CRT, it can be easily deduced that:

$$n \equiv (P^d \bmod M) \pmod{pq}$$

which is exactly what was to be computed.

4 References

- `https://brilliant.org/wiki/chinese-remainder-theorem/`
- `https://www.di-mgt.com.au/crt_rsa.html`