Massachusetts Institute of Technology — Handout R5
6.857: Network and Computer Security — March 6, 2020
Professors Ronald L. Rivest and Yael Tauman Kalai — Jake Gasparich

Recitation 5: RSA, OAEP, and CRT

1 RSA Review

1.1 Textbook RSA

Key Generation - Public Key = (n, e) where $n = p * q$ (p and q are large primes) and e is a number that is coprime to $\varphi(n)$[1].
Private Key = d where $d = e^{-1} \mod \varphi(n)$

Encryption - $y = x^e \mod n$

Decryption - $x = y^d \mod n$

RSA Assumption - given $n, e, x^e \mod n$, it is hard to compute x.

If RSA Assumption holds, Textbook RSA is a trapdoor permutation family.

1.2 CPA Secure Version of RSA

Textbook RSA is not CPA secure since it is deterministic.

Key Generation - Same as textbook RSA

Encryption - Choose r in $\mathbb{Z}_n^*$. Output $(c_1, c_2) = (r^e \mod n, H(r) \oplus m)$ [2]

Decryption - $r = c_1^d \mod n$. $m = H(r) \oplus c_2$

1.3 OAEP

In order to make RSA CCA secure, we use Optimal Asymmetric Encryption Padding (OAEP).

Key Generation - Same as textbook RSA

Encryption - $y = (pad_r(m))^e \mod n$
$pad_r(m) = (G(r) \oplus (m||0^{k_1}))||(r \oplus H(G(r) \oplus (m||0^{k_1})))$
More simply, $pad_r(m) = (x_0||x_1)$, where $x_0 = G(r) \oplus (m||0^{k_1})$ and $x_1 = (r \oplus H(x_0))$ [3]

Decryption - $x = y^d \mod n$
If x does not contain k_1 consecutive 0's, REJECT decryption. (For CCA Security Decryption Oracle).
Otherwise, $m = pad_r^{-1}(x)$

Note that OAEP makes the decryption oracle completely useless in the CCA security game since the probability of guessing an x whose decryption will contain k_1 consecutive 0's is negligible as we increase k_1 and assuming we are in the Random Oracle Model.

With no decryption oracle, the Adversary has no means of breaking the scheme, and thus, RSA with OAEP is CCA secure.

[1] $\varphi(n)$ is the number of integers in $\mathbb{Z}_n$ that are relatively prime to n, in this case $(p-1)(q-1)$.
[2] H is a hash function in the random oracle model
[3] G is also a hash function in the random oracle model

2 Chinese Remainder Theorem

The Chinese Remainder Theorem: If $m_1, m_2, ..., m_k$ are pairwise relatively prime integers, then the congruence equations $x = a_i \mod m_i$ for each $1 \leq i \leq k$ has a unique solution modulo $\prod_{i=1}^{k} m_i$.

2.1 Proof

Let $M = \prod_{i=1}^{k} m_i$. Let $N_i = M/(m_i)$ for each $1 \leq i \leq k$.

Chinese Remainder Theorem says that a solution to all congruence equations is $x = \sum_{i=1}^{k}(N_i * x_i * a_i) \mod M$. This is true since for a given i, for all $j \neq i$, $N_j = 0 \mod m_i$, since N_j was constructed as the product of all $m_i' s$ except j.

Therefore, for all i, $x = (N_i * x_i * a_i) \mod m_i$. Because all m_i are pairwise relatively prime, $N_i * x_i = 1 \mod m_i$. Thus, $x = a_i \mod m_i$ for all i.

2.2 Numeric Example

$x = 3 \mod 10$, $x = 4 \mod 7$, $x = 2 \mod 9$. Solve for smallest positive x.

$N_1 = 7 * 9 = 63$, $N_2 = 10 * 9 = 90$, $N_3 = 10 * 7 = 70$. Next, we must solve $N_i * x_i = 1 \mod m_i$ for each i. $63 * x_1 = 1 \mod 10$ gives $x_1 = 7$. $90 * x_2 = 1 \mod 7$ gives $x_2 = -1$. $70 * x_3 = 1 \mod 9$ gives $x_3 = 4$.

Now, we show that $x = \sum_{i=1}^{k}(N_i * x_i * a_i) \mod M$ is equal to $63 * 7 * 3 + 90 * (-1) * 4 + 70 * 4 * 2 = 1523$ which equals $263 \mod (10*7*9)$. Therefore, 263 is the smallest positive solution to the congruence equations.