Week 4

Lecture 2
Properties of Numbers IV
Proof of RSA Encryption

Udaya Parampalli

School of Computing and Information Systems
University of Melbourne

Lecture 1
Public Key Cryptography: Diffie-Hellman Protocol and RSA

Lecture 2
Properties of Numbers IV

Workshop 3: Workshops based on Lectures in Week 3

Quizz 4

2.1 Proof of RSA Encryption

Recap

- Numbers, Divisibility, Mod Operation, GCD, Extended GCD
- Inverse Mod n
- Properties Euler's Phi (ϕ)Function
- $\phi(p) = p - 1$, for any prime p.
- $\phi(p^a) = p^{a-1}(p-1)$, for any prime p and any integer $a \geq 1$.
- $\phi(pq) = (p-1)(q-1)$, for any two primes p and q.
- In fact, $\phi(mn) = \phi(m)\phi(n)$, for any two numbers which are relatively prime.

let $\mathbf{Z}_n^\star$ be set of numbers from 1 to $n-1$ but are relatively prime.

Theorem

If $a \in \mathbf{Z}_n^\star$, *then* $a^{\phi(n)} = 1 \pmod{n}$.

Recap:Fermat's Theorem

Theorem

Let p be a prime number, then if $gcd(a, p) = 1$, then

$$a^{p-1} = 1 \ (mod \ p).$$

This is the particular case of Euler's Theorem when n is prime.

Fermat's Little Theorem

Theorem

Let p be a prime number,

$$a^p = a \ (mod \ p), \ \textit{for any integer } a.$$

When a is relatively prime, the theorem follows from the Fermatss theorem. When a is multiple of p, the result is trivially true.

Recap:Chinese Remainder Theorem (CRT)

Let n_1, n_2 be pair-wise relatively prime integers, he system of simultaneous congruences

$$x \equiv a_1 \ (mod \ n_1),$$

$$x \equiv a_2 \ (mod \ n_2),$$

has a unique solution modulo $n = n_1 \ n_2$.

2.1 Proof of RSA Encryption.

RSA:Key Generation by entities

Before starting any transactions, Alice(A) and Bob (B) will set up the following key initializations.
Alice will do the following:

1. Generate two large and distinct primes p_A and q_A of almost equal size.
2. Compute $n_A = p_A q_A$ and $\phi_A = (p_A - 1)(q_A - 1)$.
3. Select a random integer e_A, such that $GCD[e_A, \phi_A] = 1$.
4. Compute the integer d_A such that

$$e_A d_A \equiv 1 \ (mod \ \phi_A).$$

   (Use Extended Euclidean Algorithm).

5. **Alice's Public key is** (n_A, e_A)**.**
   Alice's Private key is d_A.

Similarly, Bob will also initialize the key parameters. Let
Bob's Public key be (n_B, e_B) and
Bob's Private key be d_B,

RSA Public encryption

Here we assume that Bob wants to send a message to Alice.
Encryption at B

1. Get A's Public Key (n_A, e_A).
2. Choose a message M as an integer in the interval $[0, n_A - 1]$.
3. Compute $c = M^{e_A}\ (mod\ n_A)$.
4. Send the cipher text c to A.

Decryption at A

1. To recover m compute $M = c^{d_A}\ mod\ n_A$ using the secret d_A.

Proof of RSA Decryption

Since $e_A d_A \equiv 1 \ (mod \ \phi_A)$, by the extended Euclidean algorithm it is possible to find k such that

$$e_A d_A = 1 + k\phi_A = 1 + k(p_A - 1)(q_A - 1).$$

(Run Extended Euclidean algorithm on $(e_A, \phi(n_A))$ or $(d_A, \phi(n_A))$.)
From Fermat' theorem we get,

$$M^{p_A - 1} \equiv 1 \ (mod \ p_A).$$

Hence,

$$M^{e_A d_A} \equiv M^{1+k(p_A-1)(q_A-1)} \equiv M \ (M^{(p_A-1)})^{(q_A-1)} \equiv M \ (mod \ p_A).$$

Similarly,

$$M^{e_A d_A} \equiv M^{1+k(p_A-1)(q_A-1)} \equiv M \ (M^{(q_A-1)})^{(p_A-1)} \equiv M \ (mod \ q_A).$$

Since, p_A and q_A are distinct primes, it follows from Chinese Remainder Theorem that

$$M^{e_A \ d_A} \equiv M \ (mod \ n_A).$$

This implies,

$$c^{d_A} = (M^{e_A})^{d_A} \equiv M \ (mod \ n_A).$$

More serious proof of RSA Decryption

Note that we need to prove

$$(M^{e_A})^{d_A} = M^{e_A\ d_A} = M \ mod \ n_A.$$

If M is relatively prime to n_A, then this implies $(M, p_A) = (M, q_A) = 1$. Then the arguments in the previous slides prove the result.
You can also see this as an application of Eulers's theorem. Note that,

$$e_A d_A = 1 + k\phi_A = 1 + k(p_A - 1)(q_A - 1). \tag{1}$$

Then

$$M^{e_A\ d_A} = M^{1+k\phi_A} = M \ M^{k\phi_A} = M \ (M^{\phi_A})^k = M$$

as $M^{\phi_A} = 1 \ mod \ n_A$ (Eulers's theorem).
However, again note that to be able to use Fermat's or Euler's theorem, we need $(M, n_A) = 1$.

What if M is not relatively prime to n?

Note that the probability that M is not relatively prime to n_A is very small $(1/p_A + 1/q_A - 1/(p_A q_A))$. If we just ignore this possibility we are done. But, if you are serious and want to prove the RSA result for all $M < n_A$, then see the following.

Case when M is not relatively prime to n_A.

In this case M is divisible by either p_A or q_A. If it is divisible by both p_A and q_A, then $M = \ 0 \ mod \ n_A$ and hence the RSA result is trivially true. Then with out loss of generality assume that p_A divides M and hence we can write $M = c \ p_A$. Then we must have $(M, q_A) = 1$ (Otherwise, M is also multiple of q_A and hence identically equal to $0 \ mod \ n_A$).

Now we can use Fermat's theorem

$$M^{(q_A - 1)} = 1 \ mod \ q$$

Then taking $(k(p_A - 1))^{th}$ power on either side of the above equation, we get,

$$M^{k(p_A-1)(q_A-1)} = 1 \ mod \ q_A,$$

where k is as in (1). This implies

$$M^{k(p_A-1)(q_A-1)} = 1 + k' \ q_A,$$

for some k'. Multiplying each side by $M = cp_A$, we get

$$M^{k(p_A-1)(q_A-1)+1} = (1+k' \ q_A)M = M+k' \ (c \ p_A) \ q_A = M+k'' \ n_A.$$

Taking $mod \ n_A$ on both sides gives the result.

Lecture 1
Public Key Cryptography: Diffie-Hellman Protocol and RSA

Lecture 2
Properties of Numbers IV

Workshop 3: Workshops based on Lectures in Week 3

Quizz 4