[CS304] Introduction to Cryptography and Network Security

Course Instructor: Dr. Dibyendu Roy — Winter 2022-2023
Scribed by: Akshay (202051018) — Lecture (Week 11)

1 Euler's Theorem

If gcd(a,m) = 1 then :
$a^{\phi(m)} \equiv 1 \ mod \ m$
where, $\phi(m)$ is Euler's totient function
$S = \{x \mid gcd(x, m) = 1\}$
$= \{s_1, s_2, ..., s_{\phi(m)}\}$

gcd(s_i, m) = 1 (obvious)
Considering another set:
$S_1 = \{a.s_1, a.s_2, ..., a.s_{\phi(m)}\}$
$a.s_i \not\equiv a.s_j \ mod \ m$ (elements in S_1 are also distinct like in S)

$|S| = \phi(m)$
$|S_1| = \phi(m)$
Since, s_i (from set S) is co-prime to m, then $a.s_i$ (exist in set S_1) is also co-prime to m (because no factor can be taken out from a by m since gcd(a,m) = 1).
In nutshell, we can say some element of set S is equivalent to some element of S_1 :
$\implies s_i \equiv a.s_j \ mod \ m$

$\Pi_{i=1}^{\phi(m)} s_i \equiv \Pi_{j=1}^{\phi(m)} a.s_j \ mod \ m$
$\implies \Pi_{i=1}^{\phi(m)} s_i \equiv a^{\phi(m)}.\Pi_{j=1}^{\phi(m)} s_j \ mod \ m$
Inverse of each element exists (because of gcd being 1 with m for all elements), so we can cancel equal terms from both sides.
$\implies a^{\phi(m)} \equiv 1 \ mod \ m$

2 Fermat's Theorem

If p is a prime number and p does not divide integer a then:

$$a^{p-1} \equiv 1 \ mod \ p$$

(Derived from Euler's theroem, as $\phi(m) = m - 1$ when m is prime)
Also,

$$a^p = a \ mod \ p$$

(This one is true even when p divides a)

3 RSA Cryptosystem

Few facts :

1. If gcd(a,m) = 1 then $a^{\phi(m)} \equiv 1 \ mod \ m$
2. $a^{p-1} \equiv 1 \ mod \ p$

Designed by Rivest, Shamir and Adleman in 1977.

- n = pq   here p,q are primes
- Plaintext space = $\mathbb{Z}_n$
  Ciphertext space = $\mathbb{Z}_n$
- Key space
  $= \{K = (n, p, q, e, d) \mid ed \equiv 1 \ mod \ \phi(n)\}$
- Encryption:
  K = (n,p,q,e,d)
  E(x,K) = C
  C = E(x,K) = $x^e \ mod \ n$
- Decryption:
  Dec(C,K) = x
  x = Dec(c,K) = $c^d \ mod \ n$

Proof:

$$ed \equiv 1 \ mod \ \phi(n)$$
$$\implies ed - 1 = t.\phi(n)$$
$$1 = e.d + t_1\phi(n)$$
$$1 = gcd(e, \phi(n)) = e.d + t_1\phi(n)$$

Enc: $C = x^e \ mod \ n$
Dec: $x = c^d \ mod \ n$
$c^d = (x^e)^d \ mod \ n = x^{ed} \ mod \ n$
Also, $e.d \equiv 1 \ mod \ \phi(n)$
$ed - 1 = t.\phi(n)$
$\implies ed = 1 + t.\phi(n)$

Now, $c^d = x^{1+t.\phi(n)} \ mod \ n$
$= x.x^{t.\phi(n)} \ mod \ n$
$= x.x^{t.[(p-1).(q-1)]} \ mod \ n$
$= x.x^{t.[(p-1).(q-1)]} \ mod \ (pq)$

We need prove that $x^{t.[(p-1).(q-1)]} \equiv \ mod \ (pq)$
Possible gcds b/w x (whose range is from 0 to pq-1) and pq (p is prime, q is prime): 1, p, q (three possibilities)

- x can have multiple of neither p nor q $\implies$ gcd = 1.
- x can have multiple of p only $\implies$ gcd = p
- x can have multiple of q only $\implies$ gcd = q
- x can not have multiple of both p and q because max value of x is pq-1

Case 1:
$gcd(x, pq) = 1$
$\implies gcd(x, p) = 1$ (because no multiple p and q in x, p is prime)
and gcd(x,q) = 1
By Euler's theorem: $x^{p-1} \equiv 1 \ mod \ p$

$x^{t(p-1)(q-1)} \ mod \ p \equiv (x^{p-1})^{t(q-1)} \ mod \ p$
$\equiv 1 \ mod \ p$ (As $x^{p-1} \equiv 1 \ mod \ p$)
Similary,
$x^{t(p-1)(q-1)} \ mod \ q \equiv (x^{q-1})^{t(p-1)} \ mod \ q$
$\equiv 1 \ mod \ q$ (As $x^{q-1} \equiv 1 \ mod \ p$)

On combining these two:
$x^{t(p-1)(q-1)} \equiv 1 \ mod \ (pq)$

Case 2, 3: $\boxed{\text{pending}}$