MATH 314 Spring 2019 - Class Notes
04/25/2019
Scribe: Sura Shiferaw

Summary: Todays topic covered are Meet-in-the-Middle attack on DES, 2DES and how a brute force attack would work and ADES introduction

El-Gamal Cryptosystem

- Alice wants to create a public key
- find a large prime p(100ish digit)
- find a primitive root (mod p)
- she picks a seacret exponent a

$$2 < a < p - 1$$

- she compute

$$\beta = \alpha^a (mod p)$$

- Her public key is (p, α, β)
- Bob want to send Alice the message $m < p$
- Bob needs to pick a secret exponent b(called the eplomoral key)
- He compute $r = \alpha^b (mod p)$ $t = m\beta^b (mod p)$
- He sends the pair (r,t) to Alice
- r is masking his secret exponent
- t is masking the actual message m
- to decrypt Alice compute

$$m = t * r^{-a} (mod p)$$

Why Does $t * r^{-a} give Alice M$?

- we know

$$t = m\beta^b (mod p)$$
$$r = \alpha^b (mod p)$$
$$t(r)^{-a} = (m\beta^b) * ((\alpha^{-ba})$$
$$= m(\alpha^{ab}) * (\alpha^{-ba})(mod p)$$
$$= m\alpha^{ab-ab} = m(mod p)$$

- If Eve wants to attack this she wants to find m
- She has to use t to get it

$$t = m\beta^b (mod p)$$
$$m = t\beta(^b)^{(-1)} (mod p)$$

- She would need to know what to divide by to get m from t.
- This is B^b to find this she needs to know b
- To find b Eve would need to solve $r = B^b (mod p)$for p
- That's the discrete log problem
- Eve could decrypt the same way Alice does if she knew
- To find a Eve would need to solve $\beta = \alpha^a (mod p)$ also the discrete log problem.

Notes:Bob has to pick a different value of b each time he send a message

- If Bob uses the same b multiple times to

$$m_1 and m_2$$

$$r_1 = \alpha^b (mod p)$$

$$r_2 = \alpha^b (mod p)$$

- Eve can immediately see that Bob used the same b because $r_1 = r_2$
- If Eve manages to figure out one message m_1 then she can compute

$$\beta^b = t_1 * m_1^{-1} (mod p)$$

- so she can find m_2

$$m_2 = t_2 * \beta^b(^{-1})(mod p)$$

- Alice public key is $(p, \alpha, \beta) = (13, 2, 8)$
- Bob wants to send a message m to Alice m=10
- He picks a random b=7
- He compute $r = \alpha^b = 2^7 (mod 13)$

$$2^2 = 4(mod 13)$$

$2^4 = 16 = 3(mod 13)$

$$2^7 = 2 * 2^2 * 2^4$$

$2 * 4 * 3 = 24(mod 13) = 11(mod 13) \quad r = 11$

- $t = m * \beta^b$

$$10 * 8^7 (mod 13)$$

$$-8 = 5(mod 13)$$

$$t = 11(mod 13)$$

- Bob sends (r,t) =(11,11)
- Alice wants to decrypt (11,11)
- she compute t*r(mod p)
- recall the exponent on r matters (mod p-1)

$$-3(mod 12) = 9(mod 12)$$

$$11 * 11^9 (mod 13) = 10^{10} (mod 13)$$

$$= 36(mod 13)$$

$$10 = m(mod 13)$$

Extra Security with El-gamal over RSA

- Suppose Alice and Bob are using RSA (n,e)
- Eve sees the ciyphertext C sent from Bob to Alice
- Eve guess the real message is m
- She can check her guess by computing $m^e (mod n)$
- If she gets(she was right!)
- Now suppose they are using El-gamal, she see the ciyphertext (r,t) being sent.
- She think the message is m
- Even if she is right and tries to encrypt it she will get a different (r,t)unless she picks the same b.

Authentication

- In the physical world we can use signatures/stamp to verify our identity.
- In the digital world we need a way to tie a message to a signature.
- We want to use cryptography to do this.

RSA signature Algorithm

- Alice has an RSA public key (n,e).
- Alice want to send Bob m and prove it is her sending the message.
- She computes $S = m^d (mod n)$
- She sends Bob the pair (m,s).
- Bob want to verify the signature he computes $S^e (mod n)$

$$S^e = m^{ed} = m(mod n)$$

- Bob accepts the signature if

$$S^e = m(mod n)$$

- Alice is the only one who could have produced such a signature