MATH 314 Fall 2019 - El Gammal

11/06/2019

Scribe: Andrew Noonan

Summary: El Gammal: A public key cryptosystem. El Gammal is used to send messages using the discrete logarithm problem as a one-way function.

1. Alice Creates a public key
   - Pick a large prime p (at least 200 digits)
   - Pick a primative root (mod p), this will be called α (mod p)
   - Pick a secret exponent k where $2 <= k < p - 1$
   - Compute $\beta \equiv \alpha^k$ (mod p)
2. Alice's public key is (p, α, β)
   - k needs to stay secret
   - Eve cannot solve $\beta \equiv \alpha^k$ (mod p)
3. Bob wants to send Alice a message M. Bob picks a secret number $b(2 <= b < p - 1)$
   - B is only used one time!
   - This is called an ephemeral key
4. Bob computes his r and t
   - $r \equiv \alpha^b$ (mod p) — Sending info about b —
   - $t \equiv M * \beta^b$ (mod p) — Sending info about M —
5. Alice receives (r, t)
   - Alice computers $r^{-k} * t$ (mod p) $= M$

Notes: Why does bob need to pick a different b each time?

1. Suppose bob always uses the same b every time
2. He sends $r \equiv \alpha^b$ (mod p) and $t \equiv M * \beta^b$ (mod P)
   - One of these times Eve manges to figure out the message
   - Since Eve knows t and M, she can solve for $\beta^b \equiv t * M^{-1}$ (mod p)
3. Now suppose bob sends another message with the same b

- $r \equiv \alpha^b$ (mod p) — this does not change! —
- $t_2 \equiv M_2 * \beta^b$ (mod p)
- Since Eve knows β^b, Even can compute $T_2 * \beta^{-1} \equiv M_2$ (mod p) without ever learning k or b!
- If bob uses a different b each time Eve would have to learn k or b to decrypt

Notice: If Eve guesses the plaintext message M

- If Alice and Bob are using RSA then Even can check her guess by computing M^e (mod n) to see if this is Bob's C.
- With El Gammal Eve can't check her guess without knowing the b that Bob used.