ElGamal cryptography

ElGamal Cryptography

- ElGamal encryption is a public-key cryptosystem.
  - *It uses asymmetric key encryption for communicating between two parties and encrypting the message.*
- Public-key cryptosystem related to D-H
- uses exponentiation in a finite field
- with security based difficulty of computing discrete logarithms, as in D-H

ElGamal Digital Signature

- Global elements q and a *(a is primitive root of q)*

<u>A generates Private/Public Key:</u>

- each user generates their key
  - chooses a secret key (Private): $\mathbf{1 < x_A < q-1}$
  - computes their **public key**: $\mathbf{y_A = a^{x_A} \bmod q}$

ElGamal Message Exchange

- Bob encrypts a message to send to A computing
  - message $\mathbf{M}$ in range $\mathbf{0 <= M <= q-1}$
    - longer messages must be sent as blocks
  - chose random integer $\mathbf{k}$, $\mathbf{1 <= k <= q-1}$
  - compute one-time key $\mathbf{K = y_A^{\,k} \bmod q}$
  - encrypt $\mathbf{M}$ as a pair of integers $(\mathbf{C_1,C_2})$ where
    - $\mathbf{C_1 = a^k \bmod q}$ // like D-H public key
    - $\mathbf{C_2 = KM \bmod q}$ // encrypted msg

ElGamal Message Exchange

- encrypt M as a pair of integers (C_1, C_2) where
  - $C_1 = a^k \bmod q$; $C_2 = KM \bmod q$
- A then recovers message by
  - recovering key K as $K = C_1^{xA} \bmod q$
    [*computing* M *as* $M = C_2 K^{-1} \bmod q$] or
  - To Recover $M = C2(C1)^{q-1-xA} \bmod q$
- a unique K must be used each time
  - otherwise result is insecure

ElGamal Example

- use field GF(19) $q=19$ and $a=10$
- Alice computes her key: a xa mod q
  - A chooses $x_A=5$ & computes $y_A=10^5 \bmod 19 = 3$
- Bob send message $m=17$ as $(11,5)$ by
  - choosing random $k=6$
  - computing $K = y_A^k \bmod q = 3^6 \bmod 19 = 7$
  - computing $C_1 = a^k \bmod q = 10^6 \bmod 19 = 11$;
  - $C_2 = KM \bmod q = 7*17 \bmod 19 = 5$

ElGamal Example ...

- Alice recovers original message by computing:
  - recover $M = C2(C1)^{q-1-xA} \bmod q$

$$= 5(11)^{19-1-5} \bmod 19$$

$$= 5 * (11)^{13} \bmod 19$$

$$= \underline{17}$$

Message retrieved = 17