Groups and Crypto

Roy McElmurry

Groups

- Algebraic building blocks used to prove all kinds of mathematical facts
- For instance, the reason why there is a quadratic, cubic and quartic equation, but no quintic equation
- Composed of a set of elements and a single binary operator that can be applied to them
- The set under the operator must obey
  - Closure
  - Associativity
  - Identity

Group Example

- Z_n^*: integers that are relatively prime to n where the operator is multiplication
  - Closure: if $a,b \in Z_n^*$ then $a*b \in Z_n^*$, since there were no factors of a or b in common with n
  - Associativity: multiplication is associative
  - Identity: 1 is the identity element, $1 * x = x$
- What are the elements of Z_p^* where p is prime

Subgroups

- Assume we have a group G comprised of a set S and an operator O
- A subgroup of G is any subset of S that is itself a group under the same operator O

Ex: Let $G=Z_{10}{}^*=<\{1,3,7,9\}, (* \bmod 10)>$, then it's subgroups are the following

  - $G_1=\{1\}$
  - $G_2=\{1,9\}$
  - $G_3=\{1,3,7,9\}$

Some Facts

- Fermat's Little Theorem: if p is prime and gcd(a,p) = 1, then $a^{p-1} = 1 \bmod p$
- Chinese Remainder Theorem Corollary:
  if p and q are co-prime then if:
  - $x = a \pmod{p}$
  - $x = a \pmod{q}$

  then $x = a \pmod{pq}$

Asymmetric Crypto (RSA)

- Choose two primes p and q and let $n=pq$
- Choose e and d such that $ed=1(\mathrm{mod}\ t)$ where $t=(p-1)(q-1)$ or more precisely $t=\mathrm{lcm}(p-1,q-1)$
- The public key is the tuple (n,e)
- The private key is the tuple (p,q,t,d)
- Encryption: $E(m,(n,e)) = m^e(\mathrm{mod}\ n)$
- Decryption: $D(c, (p,q,t,d)) = c^d(\mathrm{mod}\ n) = m^{ed}(\mathrm{mod}\ n) = m\ (\mathrm{mod}\ n) = m$

RSA Example

- Let p=5 and q=11, then n=55
- t=lcm(4,10)=20, (p-1)(q-1)=40
- Let e=3, then d=7
- The public key is (n,e)=(55,3)
- The private key is (p,q,t,d)=(5,11,20,7)

- Practice example: p=17, q=23, e=3
  - Answer: t=lcm(16,22)=176, (p-1)(q-1)=352, d=59

Symmetric Crypto (Diffie-Hellman)

- Choose two primes p and q such that $p=2q+1$
- Choose an α, such that $1 < \alpha < p-1$ and set $g=\alpha^2 \bmod p$, with $g \neq 1 \pmod p$ and $g \neq p-1 \pmod p$
  - The tuple (p,q,g) are known to everyone
- Alice chooses an $x \in Z_p^*$ such that $g^x \pmod p \neq 1, p-1$, and shares $g^x \pmod p$
- Bob chooses a $y \in Z_p^*$, and shares $g^y \pmod p$
- The shared key becomes $g^{xy} \pmod p$

DH Example

- Let $q=3$, $p=7$, then $p=2q+1$
- Let $\alpha=4$, then $g=2 \pmod 7$
- Let $x=2$ then $g^x=4 \pmod 7$
- Let $y=5$ then $g^y=4 \pmod 7$
- The shared key is then $g^{xy}=2 \pmod 7$

- Practice example: $q=5, p=11$
  - Answer (many possible): $\alpha=7$, $g=5$, $x=9$, $y=8$ $g^x=9$, $g^y=4$, key$=g^{xy}=3$

How do we get these properties?

- Privacy
  - Encryption and OAEP
- Authenticity
  - Signature and CAs, MAC
- Integrity
  - MAC
- Freshness
  - Nonces

Overview

- We follow these steps (very simplified) to securely communicate with another person
  - 1) obtain this person's public key and verify it against a CA to ensure authenticity
  - 2) Negotiate a symmetric key using the asymmetric keys to ensure privacy
    - Sign all messages to ensure authenticity and integrity
    - Include a nonce in all messages to ensure freshness
  - 3) Communicate using symmetric keys for the rest of the session
    - Use MAC on all messages to ensure integrity
    - Include nonces in all messages to ensure freshness