Asymmetric (Public Key) Encryption

Number theory (Stallings, Chapter 8)

- Prime numbers
- “Fundamental Theorem of Arithmetic”
- Fermat’s (little) Theorem (and proof)
- Euler totient function; Euler’s Theorem
- Finding prime numbers using the Miller-Rabin test
- Chinese remainder theorem
  - Going back and forth between representations
- Powers of an integer, modulo n
  - Primitive root
- Discrete logarithms
  - Complexity of best-known alg. for finding discrete log
Public Key Cryptography

- Diffie-Hellman
  - Motivation

- Terminology: “public key / private key”; “secret key”

- Requirements for public key cryptography
  1. 
  2. 
  3. 
  4. 
  5. Sometimes 
  6. 

- Note: “easy”; “infeasible”
One-way function

Trap-door one-way function

Cryptanalysis in public key algorithms

1.

2.

3.

The RSA Algorithm

First (published) algorithm for public key cryptography that could encrypt and decrypt

Considerations for computation and efficient operation

Security of RSA

1.

2.

3.

4.
Elliptic Curve Cryptography (ECC)

- Computation takes place in a finite abelian group, with group operation “addition”
  - Difficulty based on an analog of the discrete log problem

- Elliptic curves over the Real Numbers
  - Geometric description of “addition”
  - Algebraic description of “addition”

- Elliptic curves over Finite Fields
  - $E_p(a, b)$
  - $E_{2^m}(a, b)$

- Example: $E_{23}(1, 1)$
  (see Stallings, Table 10.1 for the full set of points)

- Elliptic curve over $GF(2^m)$
  - Different cubic equation
  - Different definition of addition
  - Uses polynomial arithmetic
ECC encryption / decryption example

- Many proposals for doing enc/dec; this example is perhaps the simplest

- Comparison of ECC key sizes versus RSA/DSA (see Stallings, Table 10.3)

Elliptic curve using the generator representation