# Highlights of Chapters 3-4.

### Chapter 3: Integer Factorization and RSA

# 1. Number theory concepts:

- (a) Euler's formula for pq: if p and q are distinct primes and  $g = \gcd(p-1, q-1)$ , then  $a^{(p-1)(q-1)/g} \equiv 1 \mod pq$  for all a with  $\gcd(a, pq) = 1$ .
- (b) Let p and q be distinct primes and  $g = \gcd(p-1, q-1)$ , and let d such that  $de \equiv 1 \mod (p-1)(q-1)$ . Then, the congruence  $x^e \equiv c \mod pq$  has a **unique** solution  $x \equiv c^d \mod pq$ .
- (c) Fermat witness: an integer a is a witness for the compositeness of n if  $a^n \not\equiv a \mod n$ .
- (d) Proposition (Miller-Rabin): Let p be an odd prime, with  $p 1 = 2^k q$  where q is odd. Let a be relatively prime to p. Then, one of the following is true:
  - $a^q \equiv 1 \mod p$ , or
  - one of  $a^q, a^{2q}, \ldots, a^{2^{k-1}q}$  is  $\equiv -1 \mod p$ .
- (e) Let n be an odd composite number. Then at least 75% of the numbers between 1 and n-1 are Miller-Rabin witnesses for n.
- (f) The Prime Number Theorem: Let  $\pi(x)$  be the number of primes in the interval [1, x]. Then,  $\lim_{x\to\infty} \pi(x)/(x/\ln(x)) = 1$ .
- (g) Quadratic residues: a is a QR mod p if  $x^2 \equiv a \mod p$  has a solution, a QNR otherwise. There are (p-1)/2 QR's and (p-1)/2 QNR's mod p.
- (h) Quadraic residue symbol, or Legendre symbol:  $\left(\frac{a}{p}\right)$  is 1 is a is a QR, -1 if a is a QNR, and 0 if p|a.
- (i) Quadratic Reciprocity for distinct odd primes p and q:
  - $\left(\frac{-1}{p}\right)$  is 1 if  $p \equiv 1 \mod 4$ , and -1 if  $p \equiv 3 \mod 4$ .
  - $\left(\frac{2}{p}\right)$  is 1 if  $p \equiv \pm 1 \mod 8$ , and -1 if  $p \equiv \pm 3 \mod 8$ .
  - $\binom{q}{p} = \binom{p}{q}$  if p or  $q \equiv 1 \mod 4$ , and  $\binom{q}{p} = -\binom{p}{q}$  if  $p \equiv q \equiv 3 \mod 4$ .

# 2. Cryptography:

- (a) RSA:
  - Bob picks secret primes p, q, and e with gcd(e, (p-1)(q-1)) = 1. Publishes N = pq and e. Bob also computes d such that  $ed \equiv 1 \mod (p-1)(q-1)$ .
  - Alice chooses plaintext m, computes  $c \equiv m^e \mod N$ , sends c to Bob.
  - Bob computes  $m \equiv c^d \mod N$ .
- (b) Person-in-the-middle attacks.
- (c) Fermat's primality test using Fermat witnesses.
- (d) Miller-Rabin primality test using Miller-Rabin witnesses.
- (e) Pollard's p-1 factoring algorithm:
  - N is to be factored. Set a = 2 (or some other value).
  - Compute  $a^2, (a^2)^3, (a^6)^4, \dots \mod N$ , and  $d = \gcd(a^{j!} 1, N)$ .
  - If 1 < d < N, then d is a proper divisor of N and we have factored N into smaller numbers.
- (f) Goldwasser-Micali cryptosystem:
  - Bob chooses secret p and q, choose a with  $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = -1$ , and publishes N = pq and a.
  - Alice chooses m = 0 or 1, chooses 1 < r < N, and computes  $c = r^2 \mod N$  if m = 0 and  $c = ar^2 \mod N$  if m = 1. Sends c to Bob.
  - Bob computes  $\left(\frac{c}{p}\right)$ , and m = 0 if  $\left(\frac{c}{p}\right) = 1$  and m = 1 if  $\left(\frac{c}{p}\right) = -1$ .

#### **Chapter 4: Digital Signatures**

#### 1. Number theory concepts:

(a) If p is a prime and q divides p-1, then there are elements q mod p of exact order q.

## 2. Cryptography:

- (a) RSA digital signatures:
  - Sam chooses secret primes p, q. Chooses verification exponent e with gcd(e, (p-1)(q-1)) = 1, and d with  $de \equiv 1 \mod (p-1)(q-1)$ . Publishes N = pq and e.
  - Chooses document  $D \mod N$ , and signs document  $S \equiv D^d \mod N$ . Sends (D, S) to Victor.
  - Victor verifies  $S^e \equiv D \mod N$ .
- (b) Elgamal digital signature:
  - A trusted party chooses large prime p and a primitive root  $g \mod p$ .
  - Sam chooses secret signing key  $1 \le a \le p-1$ . Compute  $A \equiv g^a \mod p$ , and publishes A.
  - Chooses 1 < k < p with gcd(k, (p-1)) = 1, a document  $D \mod p$ , and computes signature  $S_1 \equiv g^k \mod p$  and  $S_2 \equiv (D aS_1)k^{-1} \mod (p-1)$ . Sends  $(D, S_1, S_2)$  to Victor.
  - Victor verifies  $A^{S_1}S_1^{S_2} \equiv g^D \mod p$ .
- (c) DSA digital signature:
  - A trusted party chooses large primes p and q such that  $p \equiv 1 \mod q$  and an element  $g \mod p$  of exact multiplicative order q.
  - Sam chooses secret signing key  $1 \le a \le q-1$ . Compute  $A \equiv g^a \mod p$ , and publishes A.
  - Chooses 1 < k < q, a document  $D \mod q$ , and computes signature  $S_1 \equiv (g^k \mod p) \mod q$  and  $S_2 \equiv (D + aS_1)k^{-1} \mod q$ . Sends  $(D, S_1, S_2)$  to Victor.
  - Victor computes  $V_1 \equiv DS_2^{-1} \mod q$  and  $V_2 \equiv S_1S_2^{-1} \mod q$  and
  - Victor verifies  $(g^{V_1}A^{V_2} \mod p) \mod q = S_1$ .