MATHEMATICS OF ASYMMETRIC KEY CRYPTOGRAPHY

- A number of concepts from number theory are essential in the design of public-key cryptographic algorithms.
- The security of a public key cryptosystem depends on the difficulty of certain computational problems in mathematics.
- A deep understanding of the security and efficient implementation of public key cryptography requires significant background in algebra, number theory and geometry.

PRIMES

- A central concern of number theory is the study of prime numbers.
- An integer p>1 is a prime number if and only if its only divisors are ±1 and ±p.
- Any integer a>1 can be factored in a unique way as $a = p_1^{a_1} \times p_2^{a_2} \times \cdots \times p_t^{a_t}$
- where p1<p2<…pt are prime numbers and where each a_i is a positive integer. This is known as the fundamental theorem of arithmetic;

$$\begin{aligned} 91 &= 7 \times 13 \\ 3600 &= 2^4 \times 3^2 \times 5^2 \\ 11011 &= 7 \times 11^2 \times 13 \end{aligned}$$

- If P is the set of all prime numbers, then any positive integer can be written uniquely in the following form: $a = \prod_{p \in P} p^{a_p} \quad \text{where each } a_p \geq 0$
- The right-hand side is the product over all possible prime numbers p; for any particular value of a, most of the exponents a_p will be 0.
- The value of any given positive integer can be specified by simply listing all the nonzero exponents in the foregoing formulation.

The integer 12 is represented by $\{a_2 = 2, a_3 = 1\}$.
The integer 18 is represented by $\{a_2 = 1, a_3 = 2\}$.
The integer 91 is represented by $\{a_7 = 1, a_{13} = 1\}$.

- Multiplication of two numbers is equivalent to adding the corresponding exponents. Given $a = \prod_{p \in \mathrm{P}} p^{a_p}, \; b = \prod_{p \in \mathrm{P}} p^{b_p}.$
- Define k=ab . We know that the integer k can be expressed as the product of powers of primes: $: k = \prod_{p \in P} p^{k_p}.$

- It follows that $k_p = a_p + b_p$ for all $p \in P$

$$k = 12 \times 18 = (2^2 \times 3) \times (2 \times 3^2) = 216$$
$$k_2 = 2 + 1 = 3; k_3 = 1 + 2 = 3$$
$$216 = 2^3 \times 3^3 = 8 \times 27$$

- Any integer of the form p^n can be divided only by an integer that is of a lesser or equal power of the same prime number, p^j with j<=n. Thus, we can say the following. Given $a = \prod_{p \in P} p^{a_p}, b = \prod_{p \in P} p^{b_p}$

- It is easy to determine the greatest common divisor of two positive integers if we express each integer as the product of primes. If a|b, then $a_p \leq b_p$ for all p.

$$a = 12; b = 36; 12|36$$
$$12 = 2^2 \times 3; 36 = 2^2 \times 3^2$$
$$a_2 = 2 = b_2$$
$$a_3 = 1 \leq 2 = b_3$$
Thus, the inequality $a_p \leq b_p$ is satisfied for all prime numbers.

$$300 = 2^2 \times 3^1 \times 5^2$$
$$18 = 2^1 \times 3^2$$
$$\gcd(18, 300) = 2^1 \times 3^1 \times 5^0 = 6$$

PRIMALITY TESTING

- For many cryptographic algorithms, it is necessary to select one or more very large prime numbers at random. Thus, we are faced with the task of determining whether a given large number is prime.
- A **primality test** is an algorithm for determining whether an input number is prime. Among other fields of mathematics, it is used for cryptography.
- Primality tests do not generally give prime factors, only stating whether the input number is prime or not.

MILLER-RABIN ALGORITHM

- The algorithm due to Miller and Rabin is typically used to test a large number for primality.
- any positive odd integer n>=3 can be expressed as $n - 1 = 2^k q$ with $k > 0$, q odd
- To see this, note that n-1 is an even integer.

- Then, divide (n-1) by 2 until the result is an odd number q, for a total of k divisions.

TWO PROPERTIES OF PRIME NUMBERS

Two Properties of Prime Numbers The **first property** is stated as follows: If p is prime and a is a positive integer less than p, then $a^2 \bmod p = 1$ if and only if either $a \bmod p = 1$ or $a \bmod p = -1 \bmod p = p - 1$. By the rules of modular arithmetic $(a \bmod p)(a \bmod p) = a^2 \bmod p$. Thus, if either $a \bmod p = 1$ or $a \bmod p = -1$, then $a^2 \bmod p = 1$. Conversely, if $a^2 \bmod p = 1$, then $(a \bmod p)^2 = 1$, which is true only for $a \bmod p = 1$ or $a \bmod p = -1$

The **second property** is stated as follows: Let p be a prime number greater than 2. We can then write $p - 1 = 2^k q$ with $k > 0$, q odd. Let a be any integer in the range $1 < a < p - 1$. Then one of the two following conditions is true.

1. a^q is congruent to 1 modulo p. That is, $a^q \bmod p = 1$, or equivalently, $a^q \equiv 1 \pmod p$.
2. One of the numbers $a^q, a^{2q}, a^{4q}, \ldots, a^{2^{k-1}q}$ is congruent to -1 modulo p. That is, there is some number j in the range $(1 \le j \le k)$ such that $a^{2^{j-1}q} \bmod p = -1 \bmod p = p - 1$ or equivalently, $a^{2^{j-1}q} \equiv -1 \pmod p$.

ALGORITHM

```
TEST (n)
1. Find integers k, q, with k > 0, q odd, so that
   (n − 1 = 2^k q);
2. Select a random integer a, 1 < a < n − 1;
3. if a^q mod n = 1 then return("inconclusive");
4. for j = 0 to k − 1 do
5. if a^(2^j q) mod n = n − 1 then return("inconclusive");
6. return("composite");
```

FACTORIZATION

- Prime factorization (or integer factorization) is a commonly used mathematical problem often used to secure public-key encryption systems.
- A common practice is to use very large semi-primes (that is, the result of the multiplication of two prime numbers) as the number securing the encryption.

Prime factorization

- To **factor** a number N is to write it as a product of other numbers: n=a X B X C
- Note that factoring a number is relatively hard compared to multiplying the factors together to generate the number
- The **prime factorisation** of a number N is when its written as a product of primes
  - Eg. 91=7x13 ; 3600=2^4x3^2x5^2

RELATIVELY PRIME NUMBERS & GCD

- Two numbers a, b are**relatively prime** if have **no common divisors** apart from 1
  - eg. 8 & 15 are relatively prime since factors of 8 are 1,2,4,8 and of 15 are 1,3,5,15 and 1 is the only common factor
- Conversely can determine the greatest common divisor by comparing their prime factorizations and using least powers
  - eg. $300=2^1 x 3^1 x 5^2$ $18=2^1 x 3^2$ hence $GCD(18,300)=2^1 x 3^1 x 5^0=6$