PUBLIC KEY ENCRYPTION

DR. O. I. ADELAIYE

RSA

LET'S DO SOME MATHEMATICS

- Prime numbers: 2, 3, 5, 7, 11, 13, …
  - X is a prime number if it can only be divided by X or 1
    - 9 and 10 are not prime numbers
- Relatively prime numbers
  - X and Y are relatively prime if they do not have any common divider other than 1
    - 9 and 10 are relatively prime

SOME LOGIC

- The totient function $\varphi(n)$
  - Gives the number of numbers smaller than n and relatively prime to n
    - $\varphi(4) = 2$
    - $\varphi(5) = 4$
    - $\varphi(6) = 2$
    - $\varphi(10) = 4$
    - $\varphi(143) = ?$
  - If n is a prime number, then $\varphi(n) = ?$
- If n is the product of two distinct prime numbers p and q, then $\varphi(n) = (p-1)(q-1)$

MORE MATHS

- Modular arithmetic
  - *a mod n*: the rest of the division of ***a*** by ***n***
    - 5 mod 3 = 2
- Some properties
  - *(a+b) mod n = (a mod n + b mod n) mod n*
    - 13 + 17 mod 5 = 0 = (3 + 2) mod 5 =

      (13 mod 5 + 17 mod 5) mod 5
  - *(a*b) mod n = (a mod n * b mod n) mod n*
  - 7*3 mod 5 = 1 = (2 * 3) mod 5

    = (7 mod 5 * 3 mod 5) mod n
  - 7 is the multiplicative inverse of 3 (mod 5)

MORE MATHS

- X will have a multiplicative inverse mod Y if and only if X and Y are relatively prime
  - Does 4 have a multiplicative inverse mod 3?
  - Does 4 have a multiplicative inverse mod 8?
  - Does 4 have a multiplicative inverse mod 6?
    - Hint: 6=2x3 !

MORE MATHS

- Modular Exponentiation
  - $7 \bmod 5=2$, $7^2 \bmod 5=4$, $7^3 \bmod 5=3$, $7^4 \bmod 5=1$, $7^5 \bmod 5=2$, …
  - $8 \bmod 6=2$, $8^2 \bmod 6=4$, $8^3 \bmod 6=2$, $8^4 \bmod 6=4$, …
  - $8^5 \bmod 6 = 8^3 \bmod 6 = 8 \bmod 6= 2$
  - $8^3 \bmod 6 = 8^{3 \bmod 2} \bmod 6= 8 \bmod 6 = 2$
  - $8^5 \bmod 6 = 8^{5 \bmod 2} \bmod 6= 8 \bmod 6 = 2$
  - Why "mod 2"? Because $\varphi(6)=2$

AND A LITTLE MORE

- $X^y \bmod n = X^{y \bmod \varphi(n)} \bmod n$
  - Valid only when n is a prime or the product of distinct primes
- Particular case: if $y \bmod \varphi(n) = 1$
  - Then, $X^y \bmod n = X^{y \bmod \varphi(n)} \bmod n = X \bmod n$
  - Very important for RSA !

RSA

- Rivest, Shamir, Adleman
  - Use a large n such that
    - $n = p \times q$, where p and q are large prime numbers
  - Choose e relatively prime to n (3?)
    - (e,n) is the public key
  - Encrypting message m with it: $c=m^e \bmod n$
  - Choose d such that $e.d = 1 \bmod \varphi(n)$
    - (d,n) is the private key
  - Decryption: $m=c^d \bmod n$ (why)?
    - Because $c^d \bmod n=(m^e \bmod n)^d n = m^{e.d} \bmod n= m^{e.d\ \varphi(n)} \bmod n= m \bmod n$
- Works the same way when encrypting with the private key and decrypting with the public key

EN
D