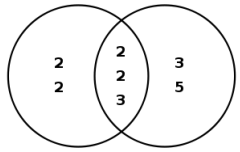
RSA AND DIGITAL CERTIFICATES
Lecture 6

COMPSCI 726
Network Defence and Countermeasures

Muhammad **Rizwan** Asghar

July 29, 2021

GREATEST COMMON DIVISOR (GCD)



- Form: **gcd(a, b)**, where a and b are integers
- gcd is the largest positive integer that divides the integers without a remainder
- Examples
  - gcd(4, 8) = 4
    - Divisors of 4 = 1, 2, **4**
    - Divisors of 8 = 1, 2, **4**, 8
  - gcd(33, 15) = 3
    - Divisors of 33 = 1, **3**, 11, 33
    - Divisors of 15 = 1, **3**, 5, 15

EULER'S PHI FUNCTION

- Form: **ϕ(n)**, where n is an integer
- An arithmetic function that **counts** the positive integers less than or equal to n that are relatively prime to n
- If n is a positive integer then ϕ(n) is the number of integers in the range 1 ≤ k ≤ n for which **gcd(k, n)=1**
- Examples
  - ϕ(2) = 1
    - gcd(1, 2) = 1 (1)
    - gcd(2, 2) = 2
  - ϕ(3) = 2
    - gcd(1, 3) = 1 (1)
    - gcd(2, 3) = 1 (2)
    - gcd(3, 3) = 3

MORE EXAMPLES

- $\phi(4) = 2$
  - gcd(1, 4) = 1 (1)
  - gcd(2, 4) = 2
  - gcd(3, 4) = 1 (2)
  - gcd(4, 4) = 4
- $\phi(5) = 4$
  - gcd(1, 5) = 1 (1)
  - gcd(2, 5) = 1 (2)
  - gcd(3, 5) = 1 (3)
  - gcd(4, 5) = 1 (4)
  - gcd(5, 5) = 5
- $\phi(11) = 10$
  - gcd(1, 11) = 1 (1)
  - gcd(2, 11) = 1 (2)
  - gcd(3, 11) = 1 (3)
  - gcd(4, 11) = 1 (4)
  - gcd(5, 11) = 1 (5)
  - gcd(6, 11) = 1 (6)
  - gcd(7, 11) = 1 (7)
  - gcd(8, 11) = 1 (8)
  - gcd(9, 11) = 1 (9)
  - gcd(10, 11) = 1 (10)
  - gcd(11, 11) = 11

EULER'S PHI FUNCTION: PROPERTIES

- **$\phi(p) = p - 1$**, where p is a prime number
  - Example
    - $\phi(11) = 10$
  - Why?

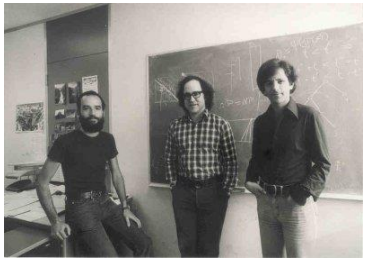
- **$\phi(pq) = \phi(p) \cdot \phi(q)$**, where p and q are coprime
  - Example
    - Let p = 5 and q = 11
    - $\phi(5 \cdot 11) = \phi(5) \cdot \phi(11) = 4 \cdot 10 = 40$

EULER'S THEOREM

- $a^{\phi(p)} \equiv 1 \pmod{p}$
  where gcd(a, p) = 1

- Example
  - Let a = 2 and p = 5, where gcd(2, 5) is 1
  - $\phi(5) = 4$
  - $2^4 \pmod{5} \equiv 16 \pmod{5} \equiv 1$

RSA



- Invented by Rivest, Shamir, and Adleman in 1978
- A public key cryptosystem
- Most popular
- Patent expired in September 2000
- Large keys (1024+ bits)

RSA: CRYPTOSYSTEM

- Generate two large prime numbers p and q
- Public parameter: $n = p \cdot q$
- Calculate: $\phi(n) = \phi(p) \cdot \phi(q) = (p - 1)(q - 1)$
- Choose e and d such that: $e \cdot d \equiv 1 \pmod{\phi(n)}$
- Public key: e
- Private key: d
- Message: m
- Enc(e, m): $c \equiv m^e \pmod{n}$
- Dec (d, c): $c^d \pmod{n}$
  $\equiv (m^e)^d \pmod{n} \equiv m^{ed \pmod{\phi(n)}} \pmod{n} \equiv m^1$

RSA: EXAMPLE

- Let $p = 3$ and $q = 11$
- Public parameter: $n = p \cdot q = 3 \cdot 11 = 33$
- Calculate: $\phi(n) = \phi(3) \cdot \phi(11) = 2 \cdot 10 = 20$
- Choose e and d such that: $3 \cdot 7 \equiv 1 \pmod{20}$
- Public key: $e = 3$
- Private key: $d = 7$
- Message: $m = 2$
- Enc(e, m): $c \equiv 2^3 \pmod{33} \equiv 8 \pmod{33}$
- Dec(d, c) : $m \equiv 8^7 \pmod{33} \equiv (2^3)^7 \pmod{33}$
  $\equiv 2^{21} \pmod{33} \equiv 2^{20} \cdot 2 \pmod{33} \equiv 1 \cdot 2 \equiv 2$

RSA SECURITY

- Security of RSA is based on integer factorisation
- Integer factorisation is same as brute-forcing
- What does it mean by x bits RSA key?
  - Public parameter n is of x bits: each of p and q is of x/2 bits
- The RSA cryptosystem with a key length of 768 bits can be broken
  - Kleinjung, Thorsten, Kazumaro Aoki, Jens Franke, Arjen Lenstra, Emmanuel Thomé, Joppe Bos, Pierrick Gaudry et al. "Factorization of a 768-bit RSA modulus." In CRYPTO 2010, vol. 6223, pp. 333-350. Springer Verlag, 2010. Link: http://eprint.iacr.org/2010/006.pdf
- A key of size more than 1024 bits is considered secure

DIGITAL SIGNATURES

- Public key algorithms can be used for digital signatures

- Signature is a hash of message encrypted with a signing key
  - Only signing key holder can create it
  - Anyone can check it using verification key

RSA: DIGITAL SIGNATURE

- Generate two large prime numbers p and q
- Public parameter: $n = p \cdot q$
- Calculate: $\phi(n) = \phi(p) \cdot \phi(q) = (p - 1)(q - 1)$
- Choose e and d such that: $e \cdot d \equiv 1 \pmod{\phi(n)}$
- **Verification** key: **e**
- **Signing** key: **d**
- **Sign(d, m)**: $S \equiv H(m)^d \pmod{n}$
- **Verify(e, m, S)**: Check if $H(m) \stackrel{?}{\equiv} S^e \pmod{n}$
  $\Rightarrow H(m) \stackrel{?}{\equiv} (H(m)^d)^e \pmod{n}$

SIGN VS. ENCRYPT

- A cryptosystem (such as RSA) can be used for signing or encrypting messages

- Always use separate keypairs for signing and encryption
  - Otherwise decrypting (hash of) a message is equivalent to signing that message

KEY BINDING

- If we do not check key binding, an adversary can substitute another key and read Alice's emails
- How do we know that a public key belongs to Alice?
- Solutions
  - X.509 certificates
  - PGP certificates

X.509 CERTIFICATES

- Use of digital certificates issued by a trusted Certificate Authority (CA)
  - E.g., VeriSign
- A digital certificate contains information to assert an identity claim
  - Version and serial number
  - Issuer and interval of validity
  - Subject's name and public key
  - Signature algorithm and signature
  - Some other fields
- Certificate Revocation List (CRL)

TO BE CONTINUED

- See the next lecture

Questions?

Thanks for your attention!