Chapter 4: Public Key Cryptography

You should not live one way in private, another in public.
— Publilius Syrus

Three may keep a secret, if two of them are dead.
— Ben Franklin

Public Key Cryptography

- Two keys
  - Sender uses recipient's **public key** to encrypt
  - Recipient uses **private key** to decrypt
- Based on "trap door one way function"
  - "One way" means easy to compute in one direction, but hard to compute in other direction
  - Example: Given p and q, product $N = pq$ easy to compute, but given N, it's hard to find p and q
  - "Trap door" used to create key pairs

Public Key Cryptography

- Encryption
  - Suppose we **encrypt** M with Bob's public key
  - Bob's private key can **decrypt** to recover M
- Digital Signature
  - **Sign** by "encrypting" with your private key
  - Anyone can **verify** signature by "decrypting" with public key
  - But only you could have signed
  - Like a handwritten signature, but way better…

RSA

RSA

- By Clifford Cocks (GCHQ), independently, **R**ivest, **S**hamir, and **A**dleman (MIT)
  - RSA is the ***gold standard*** in public key crypto
- Let p and q be two large prime numbers
- Let $N = pq$ be the **modulus**
- Choose e relatively prime to $(p-1)(q-1)$
- Find d such that $ed = 1 \bmod (p-1)(q-1)$
- **Public key** is (N,e)
- **Private key** is d

RSA

- Message M is treated as a number
- To encrypt M we compute

  $C = M^e \bmod N$
- To decrypt ciphertext C compute

  $M = C^d \bmod N$
- Recall that e and N are public
- If Trudy can factor $N=pq$, she can use e to easily find d since $ed = 1 \bmod (p-1)(q-1)$
- **Factoring the modulus breaks RSA**
  - Is factoring the only way to break RSA?

Does RSA Really Work?

- Given $C = M^e \bmod N$ we must show
  $M = C^d \bmod N = M^{ed} \bmod N$
- We'll use **Euler's Theorem:**
  If x is relatively prime to n then $x^{\varphi(n)} = 1 \bmod n$
- Facts:
  1) $ed = 1 \bmod (p - 1)(q - 1)$
  2) By definition of "mod", $ed = k(p - 1)(q - 1) + 1$
  3) $\varphi(N) = (p - 1)(q - 1)$
- Then $ed - 1 = k(p - 1)(q - 1) = k\varphi(N)$
- Finally, $\mathbf{M^{ed}} = M^{(ed - 1) + 1} = M \cdot M^{ed - 1} = M \cdot M^{k\varphi(N)} = M \cdot (M^{\varphi(N)})^k \bmod N = M \cdot 1^k \bmod N =$ **$\mathbf{M \bmod N}$**

Simple RSA Example

- Example of RSA
  - Select "large" primes $p = 11, q = 3$
  - Then $N = pq = 33$ and $(p - 1)(q - 1) = 20$
  - Choose $e = 3$ (relatively prime to 20)
  - Find d such that $ed = 1 \bmod 20$
    - We find that $d = 7$ works
- **Public key:** $(N, e) = (33, 3)$
- **Private key:** $d = 7$

Simple RSA Example

- **Public key:** $(N, e) = (33, 3)$
- **Private key:** $d = 7$
- Suppose message $M = 8$
- Ciphertext C is computed as

  $C = M^e \bmod N = 8^3 = 512 = 17 \bmod 33$
- Decrypt C to recover the message M by

  $M = C^d \bmod N = 17^7 = 410{,}338{,}673 = 12{,}434{,}505 * 33 + 8 = 8 \bmod 33$