

Outline for October 13, 2025

Reading: *text*, §10.3.2, 10.4–10.5

Due: Homework 2, due October 22; Project selection, due November 7

1. Greetings and Felicitations!

- (a) Zoom office hour on Wednesday moved to 4:00pm–4:50pm; same meeting id, password

2. RSA

- (a) Provides both authenticity and confidentiality

- (b) Based on difficulty of computing totient, $\phi(n)$, when n is difficult to factor

- (c) Go through algorithm:

Idea: Choose $n = pq$; then $\phi(n) = (p-1)(q-1)$

Choose d and compute e such that $ed \bmod \phi(n) = 1$

Now $C = M^e \bmod n$, $M = C^d \bmod n$

Public key is (e, n) ; private key is d .

- (d) Example: $p = 5$, $q = 7$; then $n = 35$, $\phi(n) = (5-1)(7-1) = 24$. Pick $d = 11$. Then $ed \bmod \phi(n) = 1$, so $e = 11$

To encipher 2, $C = M^e \bmod n = 2^{11} \bmod 35 = 2048 \bmod 35 = 18$

To decipher 18, $M = C^d \bmod n = 18^{11} \bmod 35 = 2$.

- (e) Example: $p = 53$, $q = 61$; then $n = 3233$, $\phi(n) = (53-1)(61-1) = 3120$. Pick $d = 791$. Then $e = 71$

To encipher $M = \text{RENAISSANCE}$, use the mapping A = 00, B = 01, ..., Z = 25, $\emptyset = 26$.

Then: $M = \text{RE NA IS SA NC E}\emptyset = 1704\ 1300\ 0818\ 1800\ 1302\ 0426$

So: $C = 1704^{71} \bmod 3233 = 3106 \dots$, giving $C = 3106\ 0100\ 0931\ 2691\ 1984\ 2927$

And: $M = 3106^{791} \bmod 3233 = 1704 \dots$, giving $M = 1704\ 1300\ 0818\ 1800\ 1302\ 0426$

3. Cryptographic Checksums

- (a) Function $y = h(x)$: easy to compute y given x ; computationally infeasible to compute x given y

- (b) Variant: given x and y , computationally infeasible to find a second x' such that $y = h(x')$

- (c) Keyed vs. keyless

4. Digital Signatures

- (a) Judge can confirm, to the limits of technology, that claimed signer did sign message

- (b) RSA digital signatures: sign, then encipher, then sign