Lecture 14: Cryptography

Date: October 2, 2019.

Extended GCD Algorithm

Theorem 1 (Bézout)**.** *For any integers a, b, $\gcd(a, b)$ is a linear combination of a and b, i.e., there are integers s, t such that $\gcd(a, b) = sa + tb$.*

To compute $\gcd(a, b)$, we can assume WLOG a, b are positive, and $a \geq b$.

```
gcd(a,b)
    x = a; y = b;


    while (y > 0)

        r = rem(x,y)
        x = y
        y = r



    return x
```

Question 1. Is it the case that if $ab \equiv ac \pmod{n}$ then $b \equiv c \pmod{n}$?

Proposition 2. *For any integers a, b, c, n, if $\gcd(a, n) = 1$ and $ab \equiv ac \pmod{n}$ then $b \equiv c \pmod{n}$.*

Euler's Theorem

Relatively Prime: a is relatively prime to n if $\gcd(a, n) = 1$. $\mathbb{Z}_n^* = \{a \mid 0 \leq a < n \text{ AND } \gcd(a, n) = 1\}$.

Euler's Function: $\phi(n) = |\mathbb{Z}_n^*|$

Proposition 3.

1. *For a prime p, $\phi(p) = p - 1$.*
2. *For primes p, q, $\phi(pq) = (p - 1)(q - 1)$.*

Theorem 4 (Euler)**.** *If* $\gcd(k, n) = 1$ *then*

$$k^{\phi(n)} \equiv 1 \pmod{n}$$

Proposition 5. *For any (positive) integers* a, b, c, n *such that* $\gcd(c, n) = 1$ *and* $a \equiv b \pmod{\phi(n)}$ *then* $c^a \equiv c^b \pmod{n}$*.*

Public Key Encryption (RSA) [Rivest-Shamir-Adelman 76/Cocks 73]

Messages: Each letter corresponds to a number, and message is the number obtained by concatenating all these digits.

Receiver: Picks (large) primes p, q and $e \in \mathbb{Z}^*_{\phi(n)}$, where $n = pq$. Also computes d (secret key) such that $de \equiv 1 \pmod{\phi(n)}$. "Publishes" (n, e).

Sender: To send a message $M \in \mathbb{Z}^*_n$, compute $C = \mathsf{rem}(M^e, n)$ and send C.

Receiver: To decrypt message C, compute $\mathsf{rem}(C^d, n)$. Now,

$$C^d \pmod{n} \equiv (M^e)^d \pmod{n} \equiv M^{ed \pmod{\phi(n)}} \pmod{n} \equiv M \pmod{n}$$