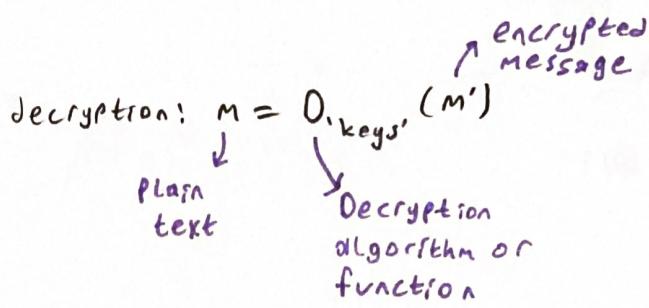
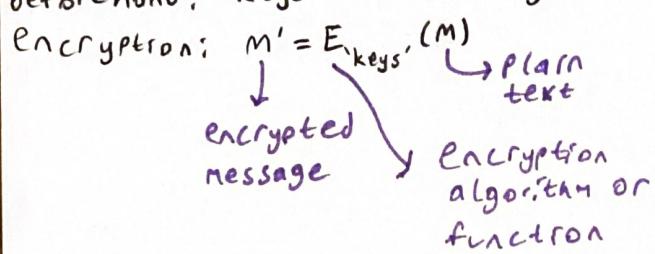


Lecture 5 - Number theory II

Encryption

beforehand: 'keys' are exchanged



Turing's code V1

For example lets take the word 'victory'. By using positions of letters lets create a new message

V i c t o r y
 $M = 22 \ 09 \ 03 \ 20 \ 15 \ 18 \ 25 \cdot 13$

an prime number that is chosen specifically for this sequence

Beforehand:

- exchange secret prime k

- Encryption: $M' = M \cdot k$

- Decrypt: $M'/k = \frac{M \cdot k}{k} = M$

** Hard to factor a product of 2 large primes

Lets say we intercept two messages $M_1' = M_1 \cdot k$ and $M_2' = M_2 \cdot k$ so $\gcd(M_1', M_2') = k$

So by using this key, we can decrypt any message, so we need a better way to encrypt messages

Turing's code V2

Beforehand:

- exchange a public prime p , and a secret prime k

- Encryption: Message as a number $M \in \{0, 1, \dots, p-1\}$
Compute $M' = \text{rem}(Mk, p)$

- Decryption: ?

Before that some definitions;

- a, b relatively prime iff $\gcd(a, b) = 1$ iff $\exists s, t$ $sa + tb = 1$

Def x is congruent to y modulo n : $x \equiv y \pmod{n}$ iff $n | (x-y)$

Ex $31 \equiv 16 \pmod{5}$ (5 divides $31-16=15$)

Def The multiplicative inverse of $(x \pmod{n})$ is a number x^{-1} , that is in interval $\{0, 1, \dots, n-1\}$ s.t. $x \cdot x^{-1} \equiv 1 \pmod{n}$

Ex $2 \cdot 3 \equiv 1 \pmod{5}$, $\underbrace{5 \cdot 5 \equiv 1 \pmod{6}}$
 $2 \equiv 3^{-1} \pmod{5}$ $5 \equiv 5^{-1} \pmod{6}$
 $3 \equiv 2^{-1} \pmod{5}$

Now let's continue our mission

- Decryption: $\underbrace{\text{rem}(Mk, p)}_{m'} \equiv Mk \pmod{p}$

If $k \cdot k^{-1} \equiv 1 \pmod{p}$, then $M'k^{-1} = \underbrace{Mk \cdot k^{-1}}_{\substack{\equiv 1 \\ \in \{0, 1, \dots, p-1\}}} \pmod{p}$

$$m = \text{rem}(M'k^{-1}, p)$$

Known-Plain text attack:

Know message m and encryption $M' = \text{rem}(Mk, p)$

$$M' \equiv Mk \pmod{p}$$

$$\gcd(m, p) = 1$$

Compute m^{-1} s.t. $mm^{-1} \equiv 1 \pmod{p}$

$$M'm^{-1} \equiv k \underbrace{mm^{-1}}_{\equiv 1} \equiv k \pmod{p}$$

Compute: $k^{-1} \pmod{p}$

Def (Euler's Totient Function);

$\phi(n)$; The number of integers in $\{1, 2, 3, \dots, n-1\}$ that are relatively prime to n

Ex $n=12$: 1 2 3 4 5 6 7 8 9 10 11 $\Rightarrow \phi(12)=4$

$n=15$: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 $\Rightarrow \phi(15)=8$

Euler's theorem: If $\gcd(n, k)=1 \Rightarrow k^{\phi(n)} \equiv 1 \pmod{n}$

Lemma 1: If $\gcd(n, k)=1$, then $nk \equiv b \pmod{n} \Rightarrow k \equiv b \pmod{n}$

*** $\gcd(n, k)=1$ iff k has a multiplicative inverse

Pf $\gcd(n, k)=1 \Leftrightarrow \exists s, t \quad n \cdot s + k \cdot t = 1 \Leftrightarrow \exists t \quad n \mid (kt-1)$
 $\Leftrightarrow kt \equiv 1 \pmod{n}$

Lemma 2: Suppose that $\gcd(n, k)=1$

Let k_1, \dots, k_r in $\{1, 2, 3, \dots, n-1\}$ denote the integers relatively prime to n ($r = \phi(n)$)

Then, $\underbrace{\{ \text{rem}(k_1 \cdot k, n), \dots, \text{rem}(k_r \cdot k, n) \}}_{\textcircled{1} \# = r} \subseteq \underbrace{\{k_1, \dots, k_r\}}_{\textcircled{2} \subseteq}$

Pf ① Suppose $\text{rem}(k_i \cdot k, n) = \text{rem}(k_j \cdot k, n)$

$$\begin{aligned} &\Rightarrow k_i \cdot k \equiv k_j \cdot k \pmod{n} \\ &\Rightarrow k_i \equiv k_j \pmod{n} \quad n \mid (k_i - k_j) \\ &\Rightarrow k_i = k_j \quad \begin{matrix} \uparrow \\ 0 \dots n-1 \end{matrix} \quad \begin{matrix} \uparrow \\ 0 \dots n-1 \end{matrix} \end{aligned}$$

Pf ② $\gcd(n, k \cdot k) = \gcd(k, \text{rem}(n, k \cdot k)) = 1$

$$\begin{gathered} \downarrow \\ \gcd(n, k) = 1 \\ \gcd(n, k_i) = 1 \end{gathered}$$

Pf. (Euler Thm)

$$1, k_1 \cdot k_2 \cdots k_r = \text{rem}(k_1, k, n) \cdot \text{rem}(k_2, k, n) \cdots \text{rem}(k_r, k, n)$$

$$\equiv k_1 \cdot k \cdot k_2 \cdot k \cdots k_r k \pmod{n}$$

$$\equiv k_1 \cdot k_2 \cdots k_r \cdot \underbrace{k}_6 \pmod{n}$$

$$1 \equiv k^r \pmod{n}$$

(3)

(little)

Fermat's theorem: Suppose p is a prime and $k \in \{1, 2, \dots, p-1\}$
Then $k^{p-1} \equiv 1 \pmod{p}$

Pf) $1, 2, \dots, p-1$ are relatively prime to $p \rightarrow \phi(p) = p-1$

$$k^{\phi(p)} \equiv 1 \pmod{p} \Rightarrow k^{p-1} \equiv 1 \pmod{p}$$

We can also use this thm. to find multiplicative inverse of k^{p-1}
 $k \cdot k^{p-2} = k^{p-1} \equiv 1 \pmod{p}$

So k^{p-2} is multiplicative inverse of k

RSA

beforehand; receiver creates public key and secret key

1. Generate two distinct p and q

2. Let $n = p \cdot q$

3. Select e s.t. $\gcd(e, (p-1)(q-1)) = 1 \Rightarrow$ public key is the pair (e, n)

4. Compute d s.t. $d \cdot e \equiv 1 \pmod{(p-1)(q-1)}$

The secret key is the pair (d, n)

Encryption: $M' = \text{rem}(M^e, n)$

Decryption: $M = \text{rem}((M')^d, n)$

$$M' = \text{rem}(M^e, n) \equiv M^e \pmod{n} \Rightarrow (M')^d \equiv M^{ed} \pmod{n}$$

$$\exists r, e \cdot d = 1 + r(p-1)(q-1)$$

$$\text{So, } (M')^d \equiv M^{ed} \equiv M \cdot M^{r(p-1)(q-1)} \pmod{n} \quad (n = pq)$$

If $M \not\equiv 0 \pmod{p}$ then $M^{p-1} \equiv 1 \pmod{p}$

If $M \not\equiv 0 \pmod{q}$ then $M^{q-1} \equiv 1 \pmod{q}$

$$n = pq : (M')^d \equiv M \cdot M^{r(p-1)(q-1)} \pmod{p}$$

$$(M')^d \equiv M \cdot M^{r(p-1)(q-1)} \pmod{q}$$

$$\text{So, } (M')^d \equiv M \pmod{p} \quad \left. \begin{array}{l} p \mid ((M')^d - M) \\ (M')^d \equiv M \pmod{q} \quad \left. \begin{array}{l} q \mid ((M')^d - M) \end{array} \right. \end{array} \right\} \frac{p \cdot q \mid ((M')^d - M)}{n \mid ((M')^d - M)}$$

$$(M')^d \equiv M \pmod{n}$$

$$M = \text{rem}((M')^d, n)$$