Lecture 5 - Number theory II

Encryption

beforehand: 'keys' are exchanged

Encryption: $m' = E_{keys}(m)$ — m': encrypted message; m: plain text; E: encryption algorithm or function

Decryption: $m = D_{keys}(m')$ — m: plain text; m': encrypted message; D: Decryption algorithm or function

Turing's code V1

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

v i c t o r y

$M = 22\,09\,03\,20\,15\,18\,25.13$ → M: prime number; 13: an prime number that is chosen specifically for this seqvence

Beforehand;
- exchange secret prime k
- Encryption: $m' = M.K$
- Decrypt: $m'/k = \frac{mk}{k} = m$

** Hard to factor a product of 2 large primes

Lets say we intercept two messages $m_1' = m_1 k$ and $m_2' = m_2 k$ 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 <u>public</u> prime P and a <u>secret</u> prime k
- Encryption: message as a number $M \in \{0, 1, \ldots, P-1\}$

  Compute $m' = rem(mk, P)$
- Decryption: ?

  Before that some definitions;

  - a, b relatively prime <u>iff</u> $gcd(a,b) = 1$ <u>iff</u> $\exists_{s,t}\ sa + tb = 1$

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

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

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

Ex $2 \cdot 3 \equiv 1 \pmod 5$, $5 \cdot 5 \equiv 1 \pmod 6$

$2 \equiv 3^{-1} \pmod 5$ $\quad 5 \equiv 5^{-1} \pmod 6$

$3 \equiv 2^{-1} \pmod 5$

Now let's continue our mission

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

If $k \cdot k^{-1} \equiv 1 \pmod p$, then $m'k^{-1} = mk \cdot k^{-1} \pmod p$

$mk \cdot k^{-1} \equiv 1 \in \{0,1,\ldots,p-1\}$

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

Known-plain text attack:

Know message m and encryption $m' = rem(mk,p)$

$m' \equiv mk \pmod p$

$gcd(m,p) = 1$

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 $ak \equiv bk \pmod n \Rightarrow a \equiv b \pmod n$

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

Pf $\gcd(n,k)=1 \Leftrightarrow \exists_{s,t}\ n\cdot s + k\cdot t = 1 \Leftrightarrow \exists_t\ n \mid (kt-1)$

$\Leftrightarrow kt \equiv 1 \pmod n$

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

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

$\Rightarrow k_i k \equiv k_j k \pmod n$

$\Rightarrow k_i \equiv k_j \pmod n$ $\quad n \mid (k_i - k_j)$ (with $0 \dots n-1$ and $0 \dots n-1$)

$\Rightarrow k_i = k_j$

Pf ② $\gcd(n, k_i k) = \gcd(k, rem(n, k_i k)) = 1$

$\gcd(n,k)=1$

$\gcd(n,k_i)=1$

Pf. (Euler Thm)

1. $k_1\cdot k_2 \cdots k_r = rem(k_1 k,n)\cdot rem(k_2 k,n) \cdots rem(k_r k,n)$

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

$\equiv k_1\cdot k_2 \cdots k_r \cdot \underbrace{k^r}_{b} \pmod n$

$1 \equiv k^r \pmod n$

Fermat's (little) theorem: Suppose p is a prime and $k \in \{1, 2, \ldots, p-1\}$

Then $k^{p-1} \equiv 1 \pmod{n}$

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

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

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. $\gcd(e, (p-1)\cdot(q-1)) = 1 \Rightarrow$ 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: $m = \text{rem}((m')^d, n)$

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

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

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 $m^{q-1} \equiv 1 \pmod{q}$

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

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

So, $(m')^d \equiv m \pmod{p}$ } $p \mid ((m')^d - m)$
$(m')^d \equiv m \pmod{q}$ } $q \mid ((m')^d - m)$] $p \cdot q \mid ((m')^d - m)$
$(m')^d \equiv m \pmod{n}$ (where $p \cdot q = n$)

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