pf for Lemma $gcd(a,b) = gcd(rem(b,a), a)$

$[m|a \wedge m|b] \Rightarrow [m|b-qa=rem(b,a) \wedge m|a]$

If $rem(b,a) \neq 0$ then $[m|rem(b,a)=b-qa$ and $m|a] \Rightarrow [m|a \wedge m|b]$ (because $b-qa+a\times q=b$ (can be obtained by linear combination))

If $rem(b,a)=0=b-qa \Rightarrow b=qa, m|a \Rightarrow m|b$ because $b=qa$ is linear combination of a.

Thm. $gcd(a,b)$ is a linear combination of a and b.

pf. (by induction) Invariant: $P(n)$ = If Euclid's Algorithm reaches $gcd(x,y)$ after n steps, then both x and y are linear combination of a and b, and $gcd(a,b)=gcd(x,y)$

Basecase: $P(0)$ is true because we have taken 0 step, a and b are linear combination of a and b, $gcd(a,b)=gcd(a,b)$

Inductive Step: Assume $P(n)$ to show $P(n+1)$

Notice that $\exists q$, $rem(y,x)=y-qx \rightarrow$ linear combination of a and b because x and y are linear combination of a and b.

Therefore, we know that after extra step, what we have reached is still a linear combination of a and b. And the Lemma has shown that the gcd of what we have reached equals to gcd of what we have started with. $\Rightarrow P(n+1)$ ✓

In a very last step of Euclid's Algorithm we achive something of this form $gcd(0,y')=y'$

Thm. $gcd(a,b)$ is the smallest positive linear combination of a and b.

Encryption

beforehand: "keys" are exchanged

encryption: $m' = E_{\text{"keys"}}(m)$

decryption: $m = D_{\text{"keys"}}(m')$

Turing's code V1.

ex) Victory $\Rightarrow m = 2209032015182513$ just added to make the whole digit into prime number

Beforehand: exchange secret prime k,

Enc: $m' = mk$

Dec: $m = m'/k$

It's hard to factor a product of 2 large primes.

$m_1' = m_1 \cdot k$, $m_2' = m_2 \cdot k$

$\gcd(m_1', m_2') = k$ because m_1 and m_2 are prime number.

Turing's code V2.

Beforehand: exchange a public prime p and secret prime k

Encryption: message as a number $m \in \{0, 1, \cdots, p-1\}$

compute $m' = \text{rem}(mk, p)$

*reminder: a, b are relative prime iff $\gcd(a,b) = 1$ iff $\exists s, t$ $sa + tb = 1$ because $\gcd(a,b)$ is the smallest linear combination of a and b

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

ex) $31 \equiv 16 \pmod{5}$ because $5 \mid (31-16)$ 31 is congruent to 16 modulo 5.

Def. The multiplicative inverse of x modulo n is a number x^{-1}, in $\{0, 1, \cdots, n-1\}$ s.t $xx^{-1} \equiv 1 \pmod{n}$

ex) $2 \cdot 3 \equiv 1 \pmod{5} \rightsquigarrow x = 2, x^{-1} = 3$ $\quad$ $5 \cdot 5 \equiv 1 \pmod{6} \rightsquigarrow x = 5, x^{-1} = 5$

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

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

Decryption: $\overbrace{\text{rem}(mk, p)}^{m'} \equiv mk \pmod{p}$

If $kk^{-1} \equiv 1 \pmod{p}$, then $m'k^{-1} \equiv m\overbrace{k \cdot k^{-1}}^{\equiv 1} \equiv \overset{\in \{0,1,\cdots,p-1\}}{m} \pmod{p}$

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

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

pf. $\gcd(n,k) = 1 \Leftrightarrow \exists s, t$ $ns + kt = 1 \Leftrightarrow \exists t$ s.t $n \mid (kt - 1) \Leftrightarrow kt \equiv 1 \pmod{n}$

Known-plaintext attack: We know message m and encryption $m' = \text{rem}(mk, p)$

$m' \equiv mk \pmod p$

$\gcd(m, p) = 1$

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

$m'm^{-1} \equiv k\overbrace{m \cdot m^{-1}}^{1} \equiv k \pmod p$

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

Def. (Euler's Totient Function) $\phi(n)$ denotes the number of integers $\{1, 2, 3, \cdots, n-1\}$ that are relatively prime to n.

ex) $n = 12$ $\quad 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11$, $\phi(12) = 4$

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

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

Lemma 1. If $\gcd(n, k) = 1$, then $ak \equiv bk \pmod n \Rightarrow a \equiv b \pmod n$

Lemma 2. Suppose that $\gcd(n, k) = 1$. Let $k_1, \cdots, k_r$ in $\{1, 2, 3 \cdots, n-1\}$ denote the integers relatively prime to n ($r = \phi(n)$)

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

pf for ① (by contradiction): Assume $\text{rem}(k_i \cdot k, n) = \text{rem}(k_j \cdot k, n) \Rightarrow k_i \cdot k \equiv k_j \cdot k \pmod n$ $\quad (k_i \cdot k = na + c,\ k_j \cdot k = nb + c)$

$\Rightarrow k_i \equiv k_j \pmod n$ $\quad (n \mid (\underset{1\sim n-1}{k_i} - \underset{1\sim n-1}{k_j})) \rightarrow$ this is possible only if $k_i = k_j$

$\Rightarrow k_i = k_j$

Therefore all the remainders are different from one another, ① $\# = r$

pf for ②: $\gcd(n, \text{rem}(k_i \cdot k, n)) = \gcd(n, k \cdot k_i)$ because $\text{rem}(k_i \cdot k, n) = k_i \cdot k - n \cdot a$

$\gcd(n, k) = 1$, $\gcd(n, k_i) = 1$ by definition $\Rightarrow \gcd(n, k \cdot k_i) = 1$

Therefore $\text{rem}(k_i \cdot k, n)$ is prime to n therefore it must be in $\{k_1, \cdots, k_r\}$ which is the set of integers relatively prime to n.

pf. (Euler's Thm) $k_1 \times k_2 \cdots \times k_r = \text{rem}(k_1 \cdot k, n) \times \cdots \times \text{rem}(k_r \cdot k, n)$

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

$\equiv k_1 \times k_2 \times \cdots \times k_r \times k^r \pmod{n}$

$\overset{a}{1} \times k_1 \times k_2 \times \cdots \times k_r \equiv k_1 \times k_2 \times \cdots \times k_r \times \overset{b}{k^r} \pmod{n}$

$1 \equiv k^r \pmod{n}$ by Lemma 1, $r = \phi(n)$ □

Fermat's (little) Thm: Suppose p is prime and $k \in \{1, 2, \cdots, p-1\}$. Then $k^{p-1} \equiv 1 \pmod{n}$

pf. $1, 2, \cdots, p-1$ are relatively prime to p. $\rightarrow \phi(p) = p-1$

$k^{\phi(p)} \equiv 1 \pmod{p}$ by Euler's thm, therefore $k^{p-1} \equiv 1 \pmod{p}$ □

$k \cdot k^{p-2} = k^{p-1} \equiv 1 \pmod{p}$ by Fermat's (little) thm and therefore $k^{-1} \equiv k^{p-2} \pmod{p}$

RSA

Beforehand: reciever creates public key and secret key

1. Generate two distinct primes p and q
2. Let $n = pq$
3. Select integer 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: $m = \text{rem}((m')^d, n)$

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

$\exists r$ $ed = 1 + r(p-1)(q-1)$ because we defined $d \cdot e \equiv 1 \pmod{(p-1)(q-1)}$

So, $(m')^d \equiv m^{ed} \equiv m\, m^{r(p-1)(q-1)} \pmod{n}$

$n = pq$. If $m \not\equiv 0 \pmod{p}$ then $m^{p-1} \equiv 1 \pmod{p}$ by Fermat's Thm

If $m \not\equiv 0 \pmod{q}$ then $m^{q-1} \equiv 1 \pmod{q}$ by Fermat's Thm

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

So, $(m')^d \equiv m \pmod{p}$, $(m')^d \equiv m \pmod{q}$ and when $m \equiv 0$, $(m')^d \equiv 0 \Rightarrow \left.\begin{array}{l} p \mid ((m')^d - m) \\ q \mid ((m')^d - m) \end{array}\right]$ because p and q are distinct prime this is possible iff $pq \mid ((m')^d - m) \Rightarrow n \mid ((m')^d - m)$

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

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