{A, B, C, D, E, F, G, H, I, J, K, L
0 1 2 3 4 5 6 7 8 9 10 11

M, N, O, P, Q, R, S, T, U
12 13 14 15 16 17 18 19 20

V, W, X, Y, Z}
21 22 23 24 25

$\mathbb{Z}_{26}$ $f(p) = (p+3) \bmod 26$

MEET YOU IN THE PARK

12 4 4 19 24 14 20 8 13 19 7 4

15 0 17 10

15 7 7 22 11 7 23 11 11 6 22 10 7

18 3 2 0 13

"PHHW BRX LQ WKH SDUN"

$f'(p) = (p-3) \bmod 26$

$f(p) = p+k \pmod{26}$

$f'(p) = p-k \pmod{26}$ Shift Cipher

$f(p) = (ap+b) \bmod 26$

$f(p) = 7p+3$ ✓

$K \rightarrow ?$ $f(10) = 7 \cdot 10 + 3 = 21 \bmod 26$

"V

Solve for x

$$3x \equiv 4 \pmod 7$$

$$\bar{3}^1 3x \equiv 4 \cdot \bar{3}^1 \pmod 7$$

$$\bar{3}^1 = \frac{1}{3} = 5$$

$$x \equiv 4 \cdot 5 \pmod 7$$

$$\equiv 6 \quad \checkmark$$

— o —

$$x \equiv 2 \pmod 3$$

$$x \equiv 3 \pmod 5$$

$$x \equiv 2 \pmod 7$$

— o —

Chinese Remainder theorem

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

$$\vdots \qquad \vdots$$

$$x \equiv a_n \pmod{m_n}$$

$\gcd(m_i, m_j) = 1 \qquad a_i \in \mathbb{Z}$

has a $\begin{matrix} ! \\ 0 \end{matrix}$ (unique) soln: $\begin{matrix} x \\ > \end{matrix}$ $(0 \le x < m)$ modulo $m_1 m_2 \ldots m_n$

$$m = m_1 m_2 \cdots m_n$$

$$M_k = \frac{m}{m_k} \quad (k = 1, 2, \ldots, n)$$

$$\gcd(m_k, M_k) = 1$$

$$\Rightarrow \exists\, y_k \in \mathbb{Z} \text{ s.t. } M_k y_k \equiv 1 \pmod{m_k}$$

$$\therefore y_k = M_k^{-1}$$

Soln. is

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_n M_n y_n \pmod{m}$$

$$\equiv a_k M_k y_k \pmod{m_k}$$

$$x \equiv a_k \pmod{m_k}$$

RSA Cryptosystem

Bob's Algo

1. Choose large prime no.s $p \neq q$
2. $n = pq$
3. Choose $e \neq 1$ s.t. $\gcd(e, (p-1)(q-1)) = 1$
4. Compute $d = e^{-1} \bmod ((p-1)(q-1))$
5. Publish $e \neq n$ → Public key
6. Keep d secret (Private key)

Alice - sending message (x) to Bob

1. Read the Public key's $e \neq n$
2. Compute $y = x^e \pmod n$
3. Send y to Bob
4. Bob recvs y from Alice & compute $z = y^d \pmod n$
5. Read z

This works if we show $z = x$

□ $y^d = x^{ed} \pmod{n}$

$\because \gcd(e, (p-1)(q-1)) = 1$

$ed = 1 \bmod ((p-1)(q-1))$

$\exists K$ s.t.

$ed = 1 + K(p-1)(q-1)$ ✓

$y^d = x^{ed} = x^{1+K(p-1)(q-1)}$

$= x \cdot x^{K(p-1)(q-1)} \pmod{n}$

$\gcd(x, p) = 1$

$\Rightarrow x^{p-1} \equiv 1 \pmod{p}$

$\gcd(x, q) = 1$

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

$y^d \equiv x \cdot (x^{p-1})^{K(q-1)} \equiv x \cdot 1 \bmod p$

$y^d \equiv x \cdot (x^{q-1})^{K(p-1)} \equiv x \cdot 1 \bmod q$

$y^d \equiv x \bmod (p \cdot q)$

$p \cdot q = n$

$y^d \equiv x \pmod{n}$