# Splitting the Modulus (SM)

Let $m, n$ be coprime positive integers. Then for any integers $x, a$,

$$\left.\begin{array}{l} x \equiv a \bmod m \\ x \equiv a \bmod n \end{array}\right\} \text{(simultaneously)} \iff x \equiv a \bmod mn$$

Pf: ($\Leftarrow$) $x \equiv a \bmod mn$

$\Rightarrow mn \mid x-a$

$\Rightarrow x \equiv a \bmod m$ $\because m \mid mn$ & $mn \mid x-a$ so by transitivity $m \mid x-a$

& $x \equiv a \bmod n$ similarly.

($\Rightarrow$) Assume $x \equiv a \bmod m$ & $x \equiv a \bmod n$

Note $x = a$ is a solution. Since $\gcd(m,n) = 1$ by CRT $x \equiv a \bmod mn$ gives all solutions.

$\blacksquare$.

For what integers is $x^5 + x^3 + 2x^2 + 1$ divisible by 6?

Want to solve

$$x^5+x^3+2x^2+1 \equiv 0 \mod 6.$$

By (SM)

$$x^5+x^3+2x^2+1 \equiv 0 \mod 2$$
$$x^5+x^3+2x^2+1 \equiv 0 \mod 3$$

Use equation 1 and plugin $x \equiv 0 \mod 2$ & $x \equiv 1 \mod 2$. In both cases

$$x^5+x^3+2x^2+1 \equiv 1 \mod 2.$$

$\therefore$ $x^5+x^3+2x^2+1$ is never divisible by 6.

# Cryptography

- The practice/study of secure commumication.

Eve

Alice ——|—— Bob

<u>NB</u>: A cryptosystem should not depend on the secrecy of the methods of encryption & decryption (except for possibly secret keys).

# Private Key Cryptography

- Agree before hand on a secret encryption & decryption key.

Ex: Caesar Cipher (ASCII Table)

Map plaintext $M$ to

$$C \equiv M+3 \mod 26 \quad (0 \le C < 26)$$

Ex:

| | | | | |
|---|---|---|---|---|
| A | P | P | L | E |
| 00 | 15 | 15 | 11 | 04 |
| 03 | 18 | 18 | 14 | 07 |
| D | S | S | O | H |

Cons of Private Key Cryptography.

- Tough to share private key before hand.
- Too many private keys to share.
- Difficult to communicate with strangers.

# Public Key Cryptography.

Analogy: Pad lock

- Easy to lock
- Difficult to unlock without a Key

Eve

Alice —— Bob

public Key e

private Key d

$M \mapsto C$

Decrypt C to M using d.

Send C

Using encryption key

- Encryption & Decryption are inverses
- d & e are different
- Only d is secret.

# Exponentiation Ciphers

Alice chooses a (large) prime $p$ and an integer $e$ satisfying

$$1 < e < p-1 \quad \& \quad \gcd(e, p-1) = 1$$

Alice makes $(e, p)$ public.

Alice computes $d$, an integer via

$$1 < d < p-1 \quad \& \quad ed \equiv 1 \mod p-1$$

Note: $d$ can be found quickly using EEA.

Note: Inverse exists $\because \gcd(e, p-1) = 1$.

To send a message $0 \leq M < p$ to Alice, Bob computes $C$ s.t.

$$0 \leq C < p \quad \& \quad C \equiv M^e \mod p$$

Bob sends $C$ to Alice & Alice computes $R \equiv C^d \mod p$ with $0 \leq R < p$.