

Math 321

Private (vs) Public

→ (ex) Affine Shift: $|Alph| = n$ must have $\gcd(a, n) = 1$

$$f(p) = (ap + k) \bmod n$$

$$f^{-1}(c) = (a^{-1}(c - k)) \bmod n$$

a^{-1} exists

Private key

(a, k, n)

b/c if known a^{-1} is "trivial" to find,

Public Information (Real world)

Step 1 make private key

Step 2 - mix the private key into a public key

- use the mixed public key to create $f(p)$

- use the private key to create $f^{-1}(c)$

Step 3 - hand out public key and $f(p)$ to everyone

Strength: is the time to unmix the public key to find private key.

RSA / Cocks

step 1: private key p, q are large primes.

Step 2: $n = pq$ $M = (p-1)(q-1)$

choose e such that $\gcd(e, M) = 1$ (so e^{-1} exists mod M)

find $d = e^{-1}$ for mod M

$$f(p) = p^e \bmod n$$

$$f^{-1}(c) = c^d \bmod n$$

Public key: (e, n)

ex

$$p = 11 \quad q = 13$$

$$n = pq = 143$$
$$m = 10 \cdot 12 = 120$$

$$\text{let } e = 7$$

$$\text{gcd}(120, 7) = 1$$

$$120 = 17 \cdot 7 + 1$$

$$1 = 1 \cdot 120 - 17 \cdot 7$$

$$7^{-1} \text{ inv is } -17 \equiv_{120} 103$$

$$\text{let } d = 103$$

(order mod 120)

$$f(p) = p^7 \pmod{143}$$

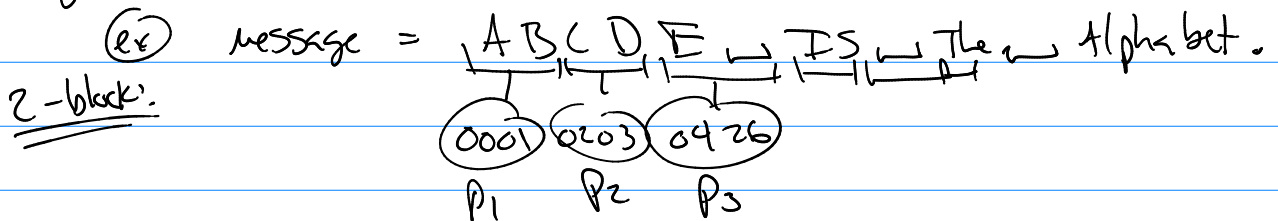
$$f^{-1}(c) = c^{103} \pmod{143}$$

Public Key $(7, 143)$

Using RSA/Cocks cryptography.

$$A = 00 \quad a = 27$$
$$B = 01 \quad b = 28$$
$$\hat{z} = 25$$
$$\text{space} = 26$$

message and block out --



$$C_1 = P_1^e \pmod{n}$$

$$C_2 = P_2^e \pmod{n}$$

i

CH5

Induction: a way to show that some $\forall n, P(n)$ are a tautology.

"Goal is to show a predicate holds for all cases"

→ If cases are finite we used proof by exhaustion

If $n=2$ & 3 & 4 , then Statement

Case 1 $n=2 \rightarrow$ show statement
Case 2 $n=3 \rightarrow$ "
Case 3 $n=4 \rightarrow$ "

Induction is to prove $\forall n_i P(n_i)$ where the cases are infinite and well ordered ① everyone can be compared (and state their order)

$n_1, n_2, n_3, n_4, n_5, \dots$ ② we always have a 1st case.

Want: $\forall n_i P(n_i)$ is a tautology

Use 3 facts:

① know $[P \wedge Q] \rightarrow P$ is true
 \rightarrow if $P \wedge Q \equiv P$ Q can be anything
 \rightarrow if $P \wedge Q \equiv T$ Q must be true

② $\left[\underbrace{P(n_i)}_{\text{show this true?}} \wedge \underbrace{\forall k (P(n_k) \rightarrow P(n_{k+1}))}_{\text{show this true?}} \right] \rightarrow \underbrace{\forall n_i P(n_i)}_{\text{want}}$ is a tautology

③ $\left[P(n_i) \wedge \underbrace{H_k(P(n_1) \wedge P(n_2) \wedge \dots \wedge P(n_k) \rightarrow P(n_{k+1}))}_{\text{want}} \right] \rightarrow \forall n_i P(n_i)$