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 "trival" to find.

Public Information (Real world)

Step1 make private key

Step2 - mix the private key into a public key
- use the mixed public key to create $f(p)$
- use the private key to create $f^{-1}(c)$

Step3 - hand out public key and $f(p)$ to everyone

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

RSA / Cocks

Step1: private key p, q are large primes.

Step2: $n = pq$ $\quad M = (p-1)(q-1)$

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

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

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

public key: (e, n)

Ex $p = 11 \quad q = 13$

$n = pq = 143$

$m = 10 \cdot 12 = 120$

let $e = 7$ $\quad \gcd(120, 7) = 1$

$120 = 17 \cdot 7 + 1$

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

7's inv is $-17 \equiv_{120} 103$ (under mod 120) $\quad$ let $d = 103$

$f(p) = p^7 \bmod 143$ $\quad$ $f^{-1}(c) = c^{103} \bmod 143$

public key $(7, 143)$

Using RSA/Cocks cryptography. -

A = 00 $\quad$ Q = 27
B = 01 $\quad$ Z = 28
Z = 25
space = 26

message and block it out --

Ex message = ABCDE ␣ IS ␣ The ␣ Alphabet.

2-block:

0001 $\quad$ 0203 $\quad$ 0426

$p_1 \quad p_2 \quad p_3$

$C_1 = p_1^e \bmod n$

$C_2 = p_2^e \bmod n$

$\vdots$

Ch 5 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 $n=2$ or 3 or 4, then [Statement]

Case 1: $n=2$ → show statement

Case 2: $n=3$ → //

Case 3: $n=4$ → //

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)

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

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

Use 3 facts:

#1 Know $[p \wedge q] \to p$ is true

a) if $p \wedge q \equiv F$ r can be anything

b) if $p \wedge q \equiv T$ r must be true

#2 $\left[P(n_1) \wedge \forall k\,(P(n_k) \to P(n_{k+1}))\right] \to \forall n_i\ P(n_i)$ is a tautology

$P(n_1)$: show this true?

$\forall k\,(P(n_k) \to P(n_{k+1}))$: show this true?

$\forall n_i\ P(n_i)$: want

#2 $\left[P(n_1) \wedge \forall k\,(P(n_1) \wedge P(n_2) \wedge \ldots \wedge P(n_k) \to P(n_{k+1}))\right] \to \forall n_i\ P(n_i)$