Lecture 6

Lemma 2.20 : $f_a(x) = x \cdot_p a$ is 1-to-1 if p is prime

Proof: By contradiction.

* Assume f_a not 1-to-1, exist

$$x \neq y, \qquad f_a(x) = f_a(y) \qquad (*)$$

* Since p is prime, a has inverse a^{-1}

* $(*) \Rightarrow \quad a^{-1} \cdot_p f_a(x) = a^{-1} \cdot_p f_a(y)$

$$\Rightarrow \quad a^{-1} \cdot_p (a \cdot_p x) = a^{-1} \cdot_p (a \cdot_p y)$$

$$\Rightarrow \quad (a^{-1} \cdot_p a) \cdot_p x = (a^{-1} \cdot_p a) \cdot_p y$$

$$\Rightarrow \quad x = y.$$

Contradiction !

* f_a must be 1-to-1.

RSA Algo

* Builds a one-way function using
  - Exponentiation mod n
  - prime numbers
  - gcd
  - multiplicative inverse in Z_n

* To prove correctness, need

  Fermat's Little Theorem

Proof of Lemma 2.19

* $a^{(i+j)} \bmod n$

$= (a^i \cdot a^j) \bmod n$

$= ((a^i \bmod n) \cdot (a^j \bmod n)) \bmod n$

$= (a^i \bmod n) \cdot_n (a^j \bmod n)$

* $(a^i \bmod n)^j \bmod n$

$= (\underbrace{(a^i \bmod n) \cdot (a^i \bmod n) \cdots (a^i \bmod n)}_{j \text{ terms}}) \bmod n$

$= (\underbrace{a^i \cdot a^i \cdots a^i}_{j \text{ terms}}) \bmod n$

$= a^{ij} \bmod n$

Exponentiation in $\mathbb{Z}_7$

$2^2 \bmod 7 = 4$

$2^3 \bmod 7 = 1$

$2^4 \bmod 7 = 2$

$2^5 \bmod 7 = 4$

$2^6 \bmod 7 = 1$ ☆

$3^2 \bmod 7 = 2$

$3^3 \bmod 7 = 6$

$3^4 \bmod 7 = (3^3 \bmod 7) \cdot 3 \bmod 7 = 4$

$3^5 \bmod 7 = (3^4 \bmod 7) \cdot 3 \bmod 7 = 5$

$3^6 \bmod 7 = (3^5 \bmod 7) \cdot 3 \bmod 7 = 1$ ☆

Corollaries of Theorem 2.21

* a, any positive integer, not multiple of p

$$a^{p-1} \bmod p = (a \bmod p)^{p-1} \bmod p$$

$$= 1$$

$\Rightarrow$ Corollary 2.22

* m, a nonnegative integer

$$m = (p-1)q + r$$

$$a^m \bmod p$$

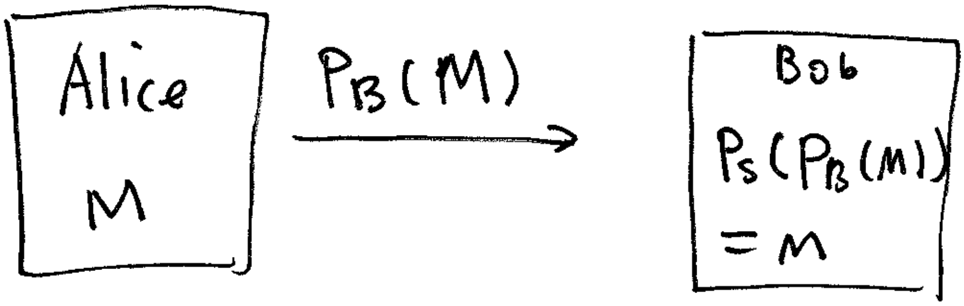
$$= a^{(p-1)q} \cdot a^r \bmod p$$

$$= \left((a^{(p-1)} \bmod p)^q \bmod p \cdot a^r \bmod p \right) \bmod p$$

$$= a^r \bmod p$$

$\Rightarrow$ Corollary 2.X1

Components of public-key Crypto system



* How to generate public key: P_B
* How to generate secret key: P_S
* How to encode plaintext using P_B
* How to decode ciphertext using P_S

RSA Correctness Proof: Step1

Show $\boxed{x \bmod p = x^{ed} \bmod p}$ (1)

Proof:

$$d = e^{-1} \bmod T$$

$$\Rightarrow ed \bmod T = 1$$

$$\Rightarrow ed = 1 + kT$$

$$= 1 + k(p-1)(q-1)$$

$$x^{ed} \bmod p$$

$$= x^{1+k(p-1)(q-1)} \bmod p$$

$$= x\,(\underbrace{x^{k(q-1)}}_{w})^{p-1} \bmod p$$

$$= x \cdot w^{p-1} \bmod p$$

$$= x \cdot (w^{p-1} \bmod p) \bmod p \quad (*)$$

Case 1: w is not multiple of p

$w^{p-1} \bmod p = 1$. Corollary 2.22

$$(*) \Rightarrow \boxed{x^{ed} \bmod p = x \bmod p.}$$

Case 2: w is a multiple of p

$\Rightarrow w^{p-1}$ is a multiple of p

$\Rightarrow \boxed{w^{p-1} \bmod p = 0}$ (★)

$(*) \Rightarrow x^{ed} \bmod p = 0$

$w = x^{k(q-1)}$, p is prime

$\Rightarrow$ x is also a multiple of p

$\Rightarrow \boxed{x \bmod p = 0}$ (★★)

(★) + (★★) $\Rightarrow$

$$\boxed{x^{ed} \bmod p = x \bmod p}$$

proved.

RSA Correctness Proof : Step 3

① $x \bmod p = x^{ed} \bmod p$

② $x \bmod q = x^{ed} \bmod q$

Show: ① + ② $\Longrightarrow$

$$x = x^{ed} \bmod n, \quad n = pq$$

---

proof:

① $\Rightarrow (x^{ed} - x) \bmod p = 0$

$\Rightarrow p \mid x^{ed} - x \quad (*)$

② $\Rightarrow (x^{ed} - x) \bmod q = 1$

$\Rightarrow q \mid x^{ed} - x \quad (**)$

$(*) + (**)$ + property of prime numbers

$\Rightarrow \quad pq \mid x^{ed} - x$

$$\Rightarrow x^{ed} - x = kpq = kn$$

$$\Rightarrow x^{ed} = kn + x$$

$$\Rightarrow x^{ed} \bmod n = x$$

$$(0 \le x < n)$$

Step 3 completed.

RSA Correctness proved.

Is RSA Secure?

* Bob: publishes e, n

* Alice: Sends $y = x^e \bmod n$

* Bob: Decodes $y^d \bmod n = x$

* Adversary can get: e, n, y

* why is it hard for him to recover x?

  - No known quick way to reverse $x^e \bmod n$, i.e. "e^{th} roots mod n"

  - How about:

    $n \Rightarrow p, q \Rightarrow d$?

    No known quick way to factor large integers