Last time

- Finish Euc. Alg.
  - examples
- Bezout's Identity
- Ext. Euc. Alg.
  - mult. inv.

Today

- Finish Ext. Euc. Alg.

- Public-Key cryptography
- RSA

Next time

- Module 3: Combinatorics

Mult. inv. of 11 (mod 26)

$\gcd(a,b) = \gcd(b, a \bmod b)$

$\gcd(a,b) = d$

$= x \cdot a + y \cdot b$

if $d=1$

↑ mult. inv. of b (mod a)

$\gcd(26,11)$: $26 = 2 \cdot 11 + 4 \iff 4 = 26 - 2 \cdot 11$ $\quad 1 = (-1) \cdot 11 + 3 \cdot (26 - 2 \cdot 11) = 3 \cdot 26 + (-7) \cdot 11$

$a_{i-1}\ b_{i-1}\ a_i\ q_{i-1}\ b_{i-1}\ r_{i-1}$ $\quad r_{i-1}\ a_{i-1}\ q_{i-1}\ b_{i-1}$ $\quad x_i\ b_{i-1}\ y_i\ a_{i-1}\ q_{i-1}\ b_{i-1}\ x_{i-1}\ a_{i-1}\ y_{i-1}\ b_{i-1}$

$\gcd(11,4)$: $11 = 2 \cdot 4 + 3 \iff 3 = 11 - 2 \cdot 4$ $\quad 1 = 1 \cdot 4 + (-1)(11 - 2 \cdot 4) = (-1) \cdot 11 + 3 \cdot 4$

$a_i\ b_i$ $\quad a_i\ q_i \cdot b_i\ r_i$ $\quad x_i\ a_i\ y_i\ b_i$

$\gcd(4,3)$: $4 = 1 \cdot 3 + 1 \iff 1 = 4 - 1 \cdot 3$ $\quad 1 = 0 \cdot 3 + 1 \cdot (4 - 1 \cdot 3) = 1 \cdot 4 + (-1) \cdot 3$

$\gcd(3,1)$: $3 = 3 \cdot 1 + 0$ $\longrightarrow$ $1 = 0 \cdot 3 + 1 \cdot 1$

$a\ b\ q\ r\ x\ y$

when remainder is zero,

$\gcd = b = 0 \cdot a + 1 \cdot b$

$a_i = b_{i-1}$

$b_i = r_{i-1} = a_{i-1} \bmod b_{i-1}$

$r_i = a_i \bmod b_i$

$q_i = \lfloor a_i / b_i \rfloor = (a_i - r_i)/b_i$

$x_{i-1} = y_i$

$y_{i-1} = x_i + (y_i) \cdot (-q_{i-1})$

$= x_i - q_{i-1} \cdot y_i$

Example: mult. inv. of 9 (mod 26)

gcd(26, 9)

⋮

$x_{i-1} = y_i$

$y_{i-1} = x_i - q_{i-1} \cdot y_i$

a	b	q	r	x	y	check
26	9	2	8	-1	3	$= 1 - 2 \cdot (-1)$	$1 = -1 \cdot 26 + 3 \cdot 9$ ✓
9	8	1	1	1	-1	$= 0 - 1 \cdot 1$	$1 = 1 \cdot 9 + (-1) \cdot 8$ ✓
8	1	8	0	0	1		$1 = 0 \cdot 8 + 1 \cdot 1$ ✓
	=		=				

gcd = 1

$1 = x \cdot a + y \cdot b$

Enc. → $y = 5 \cdot x + 11 \pmod{26}$

Dec. → $x = 21 \cdot y + 3 \pmod{26}$

Alice	Bob
P_A - public key	P_B - public key
S_A - private key	S_B - private key

two properties:

① $S(P(M)) = M = P(S(M))$

→ S & P are inverses of each other

② Can't determine S from P

Alice $\xrightarrow{M}$ Bob

① Private: $P_B(M)$ - only Bob can read

② Authentricated: $M, S_A(M)$ - Bob looks up Alice's public key P_A, applies it $S_A(M)$, and checks that $P_A(S_A(M)) = M$

③ Secure: $P_B(\langle M, S_A(M) \rangle)$

RSA

1. Pick primes p & q
2. $n = p \cdot q$
3. Pick e coprime to $(p-1)\cdot(q-1)$ ← no common factors: $\gcd(e, (p-1)\cdot(q-1)) = 1$
4. Find d, mult. inv. of e, mod $(p-1)(q-1)$
5. Public Key: (e, n)

   $P(M) = M^e \bmod n$
6. Secret Key: (d, n)

   $S(M) = M^d \bmod n$

$$(M^e)^d = (M^d)^e = M^{e \cdot d}$$

Need: $P(S(M)) = M = S(P(M))$

$M^{ed} \bmod n = M$

CS1800
Discrete Structures
Fall 2017

Lecture 14
10/5/17

Last time

- Finish Ext. Euc. Alg.
- Public-Key cryptography
- Start RSA

Today

- Finish RSA
- Start Module 3:
  Counting / Combinatorics

Next time

- Continue Counting:
  Sets & Set operations

RSA

1. Pick primes p & q
2. $n = p \cdot q$
3. Pick e coprime to $(p-1)\cdot(q-1)$
4. Find d, the mult. inv. of e, mod $(p-1)\cdot(q-1)$

   $\Rightarrow \quad d \cdot e = 1 \mod (p-1)\cdot(q-1) \quad \Rightarrow \quad d \cdot e = k(p-1)\cdot(q-1)+1$ for some int. k
5. Public Key: (e, n)

   $P(M) = M^e \mod n$
6. Secret Key: (d, n)

   $S(M) = M^d \mod n$

Note: $S(P(M)) = M^{de} \pmod n$

$P(S(M)) = M^{de} \pmod n$

$\Rightarrow$ Need $M^{de} = M \pmod n$

$$M^{de} = M^{k(p-1)(q-1)+1}$$
$$= M^{k(p-1)\cdot(q-1)} \cdot M$$

So, $M^{de} = M^{k(p-1)(q-1)} \cdot M = M \pmod n$

if $M^{(p-1)(q-1)} = 1 \pmod n$

Fermat's Little theorem

$a^p = a \pmod p$ if p is prime

$a^{p-1} = 1 \pmod p$ if p is prime and a & p are co-prime

Example

$p = 7$

$a = 3$ Consider $a \bmod p,\ a^2 \bmod p,\ \ldots,\ a^p \bmod p$

$3^1 \bmod 7 = 3 \bmod 7 = 3$

$3^2 \bmod 7 = 3 \cdot 3 \bmod 7 = 2$

$3^3 \bmod 7 = 3 \cdot 3^2 \bmod 7 = 3 \cdot 2 \bmod 7 = 6$

$3^4 \bmod 7 = 3 \cdot 6 \bmod 7 = 4$

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

$3^6 \bmod 7 = 3 \cdot 5 \bmod 7 = 1$

$3^7 \bmod 7 = 3 \cdot 1 \bmod 7 = 3$

mult. inv. of 3 $(\bmod 7)$

$a^{p-1} = 1 \pmod p$

$a^p = a \pmod p$

Claim: $M^{(p-1)\cdot(q-1)} = 1 \pmod n$ $\qquad a^{p-1} = 1 \pmod p$ $\qquad$ p - prime, a & p - coprime

case 1: M is co-prime p & q

case 2: M has common factors w/ p or q

Case 1:

$M^{p-1} = 1 \pmod p$ $\qquad M^{q-1} = 1 \pmod q$

$\Rightarrow M^{(p-1)(q-1)} = 1 \pmod p$ $\qquad M^{(p-1)(q-1)} = 1 \pmod q$

$\Rightarrow M^{(p-1)(q-1)} = k_1 \cdot p + 1$ $\qquad M^{(p-1)(q-1)} = k_2 \cdot q + 1$

So, $k_1 \cdot p = k_2 \cdot q = k \cdot p \cdot q$ for some k

So, $M^{(p-1)(q-1)} = k \cdot p \cdot q + 1$

$= k \cdot n + 1$

$\Rightarrow M^{(p-1)(q-1)} \bmod n = 1$ ✓

RSA

1. Pick primes p & q
2. $n = p \cdot q$
3. Pick e coprime to $(p-1)\cdot(q-1)$
4. Find d, the mult inv. of e, mod $(p-1)\cdot(q-1)$
   $\Rightarrow \quad d \cdot e = 1 \mod (p-1)\cdot(q-1)$
5. Public Key: (e, n)
   $P(M) = M^e \mod n$
6. Secret key: (d, n)
   $S(M) = M^d \mod n$

Note: $S(P(M)) = M^{de} \pmod n$

$P(S(M)) = M^{de} \pmod n$

$\Rightarrow$ Need $M^{de} = M \pmod n$

Operationalize

① Prime # theorem

$\pi(n) = \frac{n}{\ln n}$ — 1 in $\ln n$ #s in range 1 to n are prime

$n = 2^{1024}$

$\ln(2^{1024}) \approx 710$

② Primality testing

Security

① Must be hard to factor

② "RSA problem" — can you break RSA w/o factoring