RSA Stuff

★ Proj topics due today ★

Roots of unity WTF? (what's the formula?)

roots of unity mod 15?

												−4	−3	−2	−1	
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	: $\mathbb{Z}_{15}$
square	↓	↓	↓	↓	↓	. . .						↓	↓	↓	↓	
	0	1	4	9	1							1	9	4	1	

look at this from CRT perspective

0,0	1,1	2,2	0,3	1,4							2,1			2,4	$\mathbb{Z}_3 \times \mathbb{Z}_5$
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	$\mathbb{Z}_{15}$
↓	↓	↓	↓	↓	. . .						↓	↓	↓	↓	
0	1	4	9	1							1	9	4	1	

roots of unity are

$$(1,1) = (1,1)$$
$$(1,4) = (1,-1)$$
$$(2,1) = (-1,1)$$
$$(2,4) = (-1,-1)$$

$\boxed{\text{CRT}}$ Something is true mod pq

$\iff$ same thing true mod p & mod q

Ex: $x^2 \equiv_{pq} 1 \iff x^2 \equiv_p 1$ &

$x^2 \equiv_q 1$

Claim: If you have nontrivial sqrt unity then you can factor

$$x^2 \equiv_{pq} 1 \quad \Rightarrow \quad x^2 - 1 \equiv_{pq} 0$$

$$\Rightarrow \quad (x+1)(x-1) \equiv_{pq} 0$$

$\Rightarrow$ $(x+1)(x-1)$ is multiple of pq

prime factorization of $(x+1)(x-1)$ contains p and q

$$x \not\equiv_{pq} 1 \quad \Rightarrow \quad x - 1 \not\equiv_{pq} 0$$

$\Rightarrow$ $x-1$ is <u>not</u> multiple of pq

prime fact of $x-1$ doesn't contain <u>both</u> p & q

$$x \not\equiv_{pq} -1 \quad \Rightarrow \quad x+1 \not\equiv_{pq} 0$$

$\Rightarrow$ $x+1$ is <u>not</u> mult of pq

prime fact of $x+1$ doesn't contain <u>both</u> p & q

Note: say $N = p \cdot q$. For any x, $\gcd(\underline{x}, N)$ is either 1, p, q, or N

Strategy: identify some $\underline{x}$ that is mult of $\left.\begin{matrix} p \\ q \end{matrix}\right\}$ but not

Computing SQRT UNITY given e & d

given N, e, d: $\quad ed \equiv_{\varphi(N)} 1$

can factor N

by first computing nontriv. sqrt(1)

(then do gcd to factor)

Idea: $\quad ed - 1$ is mult of $\varphi(N)$

so $\quad w^{ed-1} \equiv_N w^0 \equiv 1$

what if $ed-1$ is even: $\quad ed-1 = 2k$

then

$$1 \equiv_N w^{ed-1} \equiv \underbrace{(w^k)}_{\text{sqrt of unity}}{}^2$$

If $ed-1$ is divisible by 4 : $\quad ed-1 = 4k$

$$1 \equiv w^{ed-1} \equiv ((w^k)^2)^2$$

In general: $\quad ed-1 = 2^s \cdot r$

$$w^r \longrightarrow w^{2r} \longrightarrow w^{4r} \longrightarrow w^{8r} \longrightarrow \cdots \longrightarrow w^{2^s r}$$

$$\hphantom{w^r \longrightarrow w^{2r} \longrightarrow w^{4r} \longrightarrow w^{8r} \longrightarrow \cdots \longrightarrow} \;\; \mathrel{\rotatebox{90}{$\equiv$}}$$

$$\hphantom{w^r \longrightarrow w^{2r} \longrightarrow w^{4r} \longrightarrow w^{8r} \longrightarrow \cdots \longrightarrow} \;\; 1$$

Claim: given N, e, m^e
hard to guess MSB of m

(because IF you could figure out MSB(m) from this information, THEN you could factor N)

Consequence: public key encryption!

public key: N, e
private key: d

to Encrypt $b \in \{0,1\}$ using public key:

- choose random $m \leftarrow \mathbb{Z}_N$
- compute $c \equiv m^e$
  $x = \boxed{MSB(m)} \oplus b$

  looks random to eavesdropper, given N, e, c
- output (c, x)

to Decrypt:

$$b = x \oplus MSB(c^d)$$