CIS 3362

10/23/~~25~~ 24

1) Quiz ~~3~~ 4 Info

2) Factoring Algorithms
   - Fermat
   - Pollard-Rho

Quiz 4

Bring Calculator - AID

Write out each step

$p = 101$

Find the Remainder when 56^{2303} is divided by 101

$\phi(101) = 101 - 1 = 100$

$56^{100} \equiv 1 \pmod{101}$ via Fermat's Thm

$56^{2303} = 56^{2300} \times 56^{3}$

$= (56^{100})^{23} \times 175{,}616$ (via calc)

$\equiv 1^{23} \times 78 \pmod{101}$ via Fermat's Thm

$\equiv \boxed{78 \pmod{101}}$

Prime Factorization, Fermat's Thm, Euler's Thm, Disc Log Problem, ϕ function, fast mod expo, Miller-Rabin Factoring Alg's.

Fermat Factoring

$$x^2 - y^2 = (x+y)(x-y)$$

$$1081 = a \times b$$

$$x^2 - y^2 = 1081 \qquad x^2 > \sqrt{1081} = 32\ldots$$

$$x^2 - 1081 = y^2 \qquad x \geq 33$$

x	$x^2 - 1081$	Is it perfect sq?
33	$33^2 - 1081 = 8$	NO
34	$34^2 - 1081 = 75$	NO
35	$35^2 - 1081 = 144$	YES

minimum integer $\rightarrow \sqrt{N}$

Works better if the 2 primes are close together!

$$35^2 - 1081 = 12^2$$

$$35^2 - 12^2 = 1081$$

$$(35+12)(35-12) = 1081$$

$$47 \times 23 \checkmark$$

Pollard - Rho Factorization

$n = x \cdot y$
$\uparrow \quad \uparrow$

```
a = 2
b = 2
while (true) {
    a = (a*a+1) % n
    b = (b*b+1) % n
    b = (b*b+1) % n
    d = gcd(a,b)
    if (d > 1 && d < n)
        return d;
    if (d == n) return FAIL;
}
```

Why a once, b twice

$s_1, s_2 \bmod n$
$s_2, s_4 \bmod n$
$s_3, s_6 \bmod n$
$s_4, s_8 \bmod n$
etc.

* We might fail

→ defining a sequence without mod grows fast

2, 5, 26, 677, ... → $s_1, s_2, s_3, \ldots$

any sequence under mod will eventually repeat!

Banking on hope that cycle size is smaller than x or y mod n.