Crypto 2 Ü3 08. NOV. 2011

Ex 8.)

Euler's criterion

Let $p > 2$ be a prime number

$c \in \mathbb{Z}_p^*$ is a QR mod p // Prop 9.2

$\Leftrightarrow c^{\frac{p-1}{2}} \equiv 1 \bmod p$

Proof:

$\boxed{\text{"}\Rightarrow\text{"}}$ (if) (Assume) c is a QR mod p (holds)

$\Rightarrow \exists x \in \mathbb{Z}_p^* : x^2 \equiv c \bmod p$ // c.f. Def. 9.1

$\Rightarrow (x^2)^{\frac{p-1}{2}} \equiv c^{\frac{p-1}{2}} \bmod p$

$\Rightarrow x^{p-1} \overset{\text{Fermat}}{\equiv} 1 \bmod p$

$\boxed{\text{"}\Leftarrow\text{"}}$ (only if) (Assume) $c^{\frac{p-1}{2}} \equiv 1 \bmod p$ (holds)

(to assure the assumption) let y be ~~PE~~ mod p

$\Rightarrow c \equiv y^j \bmod p$ // y is a generator of $\mathbb{Z}_p^*$ // Def. 7.1

$c^{\frac{p-1}{2}} \equiv (y^j)^{\frac{p-1}{2}} \overset{!}{\equiv} 1 \bmod p$

Fermat:

$\Rightarrow p-1 \mid j \cdot (p-1)/2$

$\Rightarrow j$ must be <u>even</u>!

$\exists x \in \mathbb{Z}_p^* \; x \equiv y^{j/2} \bmod p$

$\Rightarrow x^2 \equiv y^j \bmod p$

$\Rightarrow c$ is a QR mod p $\square$

Ex 9.)

Rabin cryptosystem

- Decipher $c = 1935$ given $n = 4757$

a.) find the private key by factoring

Quadratic Sieve

$\sqrt{n} = \sqrt{4757} < 69$

try $p = 67 \Rightarrow 67 \cdot 71 = 4757 \Rightarrow q = 71$

b.) Decipher $m = \sqrt{c} \bmod n$

1.) check if $p, q \equiv 3 \bmod 4$ ✓

2.) Compute square roots $\bmod p$, $\bmod q$

$k_p = \frac{p-1}{4} = 17$, $k_q = \frac{q+1}{4} = 18$

$\pm x_1 = 1935^{17} \pmod{67} = \begin{cases} 40 \\ 67 - 40 = 27 \end{cases}$

$\pm x_2 = 1935^{18} \pmod{71} = \begin{cases} 36 \\ 71 - 36 = 35 \end{cases}$

3.) find $\sqrt{c} \bmod n = m$

$f = a \cdot x + by$ solves $f^2 \equiv c \bmod n$

$a = t \cdot q$, $b = s \cdot p$

$\Rightarrow t \cdot q + s \cdot p = 1 \overset{EEA}{\Rightarrow} 1 = 17 \cdot 71 - 18 \cdot 67$
$= t \cdot q + s \cdot p$

$a = t \cdot q = 17 \cdot 71 = 1207 \bmod n$

$b = -s \cdot p = -18 \cdot 67 = -1206 \bmod n$

$m_1 = a(+x_1) + b(+x_2) = 107 \bmod n$

$m_2 = a(+x_1) + b(-x_2) = 1313 \bmod n$

$m_3 = a(-x_1) + b(+x_2) = 3444 \bmod n$

$m_4 = a(-x_1) + b(-x_2) = 4650 \bmod n$

Crypto 2 Ü3

08. NOV. 2011

last two digits must be 1:

binary: $m_1 = 0000001101011$

$m_2 = 0010100100001$

$m_3 = \ldots$

⌈ check: $\forall i : m_i^2 \equiv \underbrace{1935}_{c} \mod n$ ⌋

Ex 10.)

a.) If $x \equiv -x \pmod p$, then $x \equiv 0 \pmod p$

$-x \equiv x \pmod p$

$\overset{+x}{\iff} 0 \equiv 2x \mod p \qquad 2 \in \mathbb{Z}_p^*$

$\overset{1 \cdot 2^{-1}}{\iff} 0 \equiv x \mod p \qquad \square$

b.) Given $x, y \not\equiv 0 \mod p$ and $x^2 \equiv y^2 \mod p^2$

proof: show that $x \equiv \pm y \mod p^2$

first rewrite and use power rules

$x \equiv \pm y \pmod{p^2} \iff x \pm y \equiv 0 \pmod{p^2}$

$p^2 \mid (x^2 - y^2) \iff p^2 \mid (x+y)(x-y)$

p^2 can have 3 divisors: $\{1, p, p^2\}$

⌈ Assume for some a, b, c that ⌉

$a \mid bc$, if $\gcd(a, b) = 1 \Rightarrow a \mid c$

⌊ set $a = p^2$, $b = x - y$, $c = x + y$ ⌋

1.) If $\gcd(p^2, x-y) = 1 \Rightarrow p^2 \mid (x+y)$

$\Rightarrow x \equiv -y \pmod{p^2}$

2.) if $\gcd(p^2, x+y) = 1 \Rightarrow p^2 | (x-y) \Rightarrow \underbrace{x \equiv y \pmod{p^2}}$

3.) if $\gcd(p^2, x-y) = p^2 \Rightarrow p^2 | (x-y)$

4.) if $\gcd(p^2, x+y) = p^2 \Rightarrow p^2 | (x+y)$ $\Big\}$ $x \equiv \pm y \pmod{p^2}$

5.) if $\gcd(p^2, x-y) = p \Rightarrow p | p^2 \wedge p | (x-y)$

6.) if $\gcd(p^2, x+y) = p \Rightarrow p | p^2 \wedge p | (x+y)$ $\Big\}$ $x \equiv \pm y \pmod{p}$

but as 5.) and 6.) imply $p | (x+y) \cdot (x-y)$

$\Rightarrow x \equiv -x \pmod{p}$

$\Rightarrow x, y \equiv 0 \pmod{p}$

but $x, y \not\equiv 0 \pmod{p}$ by assumption

$\Rightarrow$ 1.), 2.), 3.), 4.) are the remaining solutions

$x \equiv \pm y \pmod{p^2}$

$\square$

c.) [on the web]