Crypto 2 Ü1 18. OKT. 2011

## Ex 1.1

a.) Compute $11^{213} \pmod{42}$

$$213_{10} \hat{=} 11010101_2$$

$$11^{213} = ((((((((11^1)^2 \cdot 11^1)^2 \cdot \cancel{11^0})^2 \cdot 11^1)^2 \cdot \cancel{11^0})^2 \cdot 11^1)^2 \cdot \cancel{11^0})^2 \cdot 11^1 \pmod{42}$$

square-multiply → s m s s m s s m s m

by table:

| | $11^{213} \bmod 42$ |
|---|---|
| s | 37 |
| m s | 1 |
| s | 1 |
| m s | 37 |
| s | 25 |
| m s | 25 |
| s | 37 |
| m | 29 |

$\Rightarrow 11^{213} \pmod{42} = \underline{\underline{29}}$

b.) $16^{512}$ $\qquad 16 \equiv -1 \pmod{17}$

$$\Rightarrow 16^{512} \pmod{17} = (-1)^{512} \pmod{17}$$
$$\equiv \underline{\underline{1}} \pmod{17}$$

Ex2.)

a.) $b_j = \alpha^j \bmod p$

$g_i = \beta \cdot \alpha^{-im} \bmod p$

$x = j + im \pmod{p-1}$

$b_j = g_i \iff \alpha^j \equiv \beta \cdot \alpha^{-im} \bmod p$

$\iff \alpha^{j+im} \equiv \beta \bmod p$

$\iff \alpha^x \equiv \beta \bmod p$ $\square$

The babystep-Giantstep-algorithm computes the discrete logarithm

b.)

As $\beta \in \mathbb{Z}_p^*$, $\alpha$ must be a generator of the cyclic ~~and~~ (multiplicative) group $\mathbb{Z}_p^*$. From Def. 7.1., we know that $\langle \alpha \rangle = \mathbb{Z}_p^*$ if $\alpha$ is a primitive element.

(group generated by $\alpha$)

c.)

$\alpha^x \bmod p \equiv \beta$, $\alpha = 3$, $p = 29$, $\beta = 13$

find an $x$ that solves $x = \log_\alpha(\beta)$

(1) $m = \lceil \sqrt{29} \rceil = 6$

| | i/j | 0 | 1 | 2 | 3 | 4 | 5 $(m-1)$ |
|---|---|---|---|---|---|---|---|
| (2) | $b_j = \alpha^j \bmod p$ | 1 | 3 | 9 | 27 | 23 | 11 |
| (3) | $g_i = \beta\alpha^{-im} \bmod p$ | 13 | 25 | 28 | 7 | 9 | 24 |

omit it

// $\alpha^{-1} \bmod p = 10$

since $3 \cdot \underline{10} - 1 \cdot 29 = 1$

$\alpha^{-im} = 10^6 \bmod 29$
$= 22$

For $(2,4) \Rightarrow$ for $b_2 = g_4 = 9$ holds

$\Rightarrow x \equiv m \cdot i + j \pmod{p-1} = 6 \cdot 4 + 2 \bmod 28 = \underline{\underline{26}}$

Crypto 2 Ü 1 18. OKT. 2011

the DL is 26

check: $3^{26} \bmod 29 = 3^{13} \cdot 3^{13} = 19 \cdot 19$

$= 13 \pmod{29}$ ✓

remark to complexity

Running $2\sqrt{p} = O(\sqrt{p})$

Brute force $\approx O(p)$

<u>Ex 3.)</u>

prove that $a^x \equiv a^y \bmod n$

$\Leftrightarrow x \equiv y \bmod \mathrm{ord}_n(a)$

with $x, y \in \mathbb{Z}$ $a \in \mathbb{Z}_n^\alpha$ $a \neq 1$ $\mathrm{ord}_n(a) = k$

"$\Rightarrow$" Let $a^x \equiv a^y \bmod n \Rightarrow a^{x-y} \equiv 1 \pmod n$

with $a^k \equiv 1 \pmod n \Rightarrow \mathrm{ord}_n(a) = k$ // smallest possible integer $k$

$\Rightarrow k \mid (x-y) \Rightarrow x \equiv y \pmod k$

$\Rightarrow x \equiv y \bmod (\mathrm{ord}_n(a))$

"$\Leftarrow$" Let $x \equiv y \bmod (\mathrm{ord}_n(a)) \Rightarrow k \mid (x-y)$

$\Rightarrow x-y = k \cdot l,\ l \in \mathbb{Z}$

$\Rightarrow a^{x-y} \equiv a^{k \cdot l} = (a^k)^l = 1^l \equiv 1 \pmod n$

$\Rightarrow a^{x-y} \equiv 1 \bmod n \Rightarrow a^x \equiv a^y \bmod n$ $\square$

Ex 4.)

Find basis $a$ for $a^{13} \equiv 17 \pmod{31}$

1.) usually a difficult problem, but 31 is prime.

Apply proposition 7.5. (p.53) to show that 17 is a primitive element mod 31.

$\Rightarrow 17^{(p-1)/p_i} \not\equiv 1 \pmod{p} \quad \forall i = 1, \dots, k$

where $p-1 = \prod_{i=1}^{k} p_i^{t_i}$ (important to remember!!)

here:

$p = 31 \Rightarrow p-1 = 30 = 2 \cdot 3 \cdot 5$

check:

$17^{\frac{30}{2}} \equiv 30, \quad 17^{\frac{30}{3}} \equiv 25, \quad 17^{\frac{30}{5}} \equiv 8$

$\not\equiv 1 \pmod{31}$

17 is a PE.

2.) Knowing that 17 is a PE mod 31:

$\exists b \quad 17^b \equiv a \pmod{31}$

$(a^{13}) \equiv a \pmod{31}$

$\Rightarrow a^{13 \cdot b - 1} \equiv 1 \pmod{31}$

with: Th. 6.2.: Let $a \in \mathbb{Z}_n^*$, then $a^{\varphi(n)} \equiv 1 \pmod{n}$

Fermat's Little theorem (p.43)

$\varphi(31) = 30$ ← prime

here: $a^{\varphi(n)} \equiv a^{30} \equiv 1 \pmod{31}$

$a^{13b-1} \equiv a^{30} \equiv 1 \pmod{31}$

Crypto 2 ü 1



$$\Leftrightarrow \quad 13 \cdot b - 1 \equiv 30 \pmod{30}$$
$$\Leftrightarrow \quad 13 b \equiv 1 \pmod{30}$$
$$b = 13^{-1} \pmod{30}$$

<u>EEA</u>: $30 = 13 \cdot 2 + 4$ $\Rightarrow 1 = 13 - 4 \cdot 3$

$13 = 4 \cdot 3 + \underline{\underline{1}}$

$= 13 - (30 - 13 \cdot 2)\, 3$

$= 13 \cdot 7 - 30 \cdot 3$

$= 13^{-1}$

$$\Rightarrow a = 17^{7} = \underline{12} \pmod{31}$$

check $12^{13} \equiv 17 \pmod{31}$