Crypto 2 Ü 2

25. OKT. 2011

Ex5.)

a) • Public domain parameters:
select an additive (/cyclic) group G
of order n with a generator P
(/primitive element a).

• Private key: some random secret
$x \in \{1, \dots, n-1\}$

• Public key: P (/a), description of G,
$y = x \cdot P$ in G (/$y = a^x$ in G)

• Encryption: - Let $m \in G$ be the message
- Choose some random secret $k \in \{1, \dots, n-1\}$
- Compute $K = k \cdot y$ in G (/ y^k)
- Generate cryptogram $C = (C_1, C_2)$
with $C_1 = k \cdot P$ (/a^k)
$C_2 = m + K$ in G (/$m \cdot k$)

• Decryption: - Compute $x \cdot C_1 = K$

$$\left[\Rightarrow x \cdot C_1 = x \cdot k \cdot P \underset{\substack{\uparrow \\ \text{commutativity}}}{=} k \cdot x \cdot P = k \cdot y = K \right] \text{in } G$$

$$\left[k \cdot P = (k-1) \cdot P + P = \underbrace{P + \dots + P}_{k \text{ addends}} \right]$$

- Recover: $m = -x C_1 + C_2 = -K + m + K \underline{\underline{= m}}$

Note: $-x C_1 = (n - x) C_1$
($/ C_1^x = K$, $m = C_1^{-x} C_2 = K^{-1} C_2$)

b.) Given : • $x \cdot C_1$, it is difficult to obtain x.

• $x \cdot C_1$ needs to be calculated efficiently.

• Commutativity

c.) „Double and Add" <-> „Square and Multiply"

$y = k \cdot P$ in G $\qquad$ $y = a^k$ in G (different Gs!)

$k = (x_l, x_{l-1}, \dots, x_0)_2 \Leftrightarrow k = \sum_{i=0}^{l} x_i \cdot 2^i \quad x_i \in \{0,1\}, x_l = 1$

$y \leftarrow P$	$y \leftarrow a$
for $i = l-1, \dots, 0$	for $i = l-1, \dots, 0$
$\quad y \leftarrow y + y$ in G	$\quad y \leftarrow y^2$ in G (mod n)
$\quad$ if ($x_i = 1$)	$\quad$ if ($x_i = 1$)
$\quad\quad y \leftarrow y + P$ in G	$\quad\quad y \leftarrow y \cdot a$ (mod n)
$\quad$ end if	$\quad$ end if
end for	end for

Ex 6.)

An irreducible polynomial is not divisible by any other polynomial

a.) $f_3(u) = u^3 + x_2 u^2 + x_1 u + x_0$, $\quad x_i \in \{0,1\}$

reducible : $f_3(u) = \begin{cases} u^k (u+1)^{3-k} & k \in \{0,1,2,3\} \\ f_2(u) \cdot u^k (u+1)^{1-k} & k \in \{0,1\} \end{cases}$

irreducible

$f_3(u)$ is irreducible if $f_3(0) = f_3(1) = 1$

if $x_0 = 0 \Rightarrow f_3(0) = 0$

$u^3 + \qquad +1 \Rightarrow f(1) = 0$

$u^3 + \qquad u + 1 \Rightarrow f(1) = 1 \Rightarrow u^3 + u + 1$ is irreducible crypto 2 Ü2

$u^3 + u^2 \quad + 1 \Rightarrow f(1) = 1 \Rightarrow u^3+u^2+1$ is irreducible
$u^3 + u^2 + u + 1 \Rightarrow f(1) = 0$

$\Rightarrow u^3+u+1$ and u^3+u^2+1 are all irreducible polynomials of degree 3.

b.) $f(u) = u^3+u+1$
$u^0 = 1, \quad u^1 = u, \quad u^2 = u^2, \quad u^3 = u+1,$
$u^4 = u^3 \cdot u = u^2+u, \quad u^5 = u^4 \cdot u = u^3+u^2 = u^2+u+1,$
$u^6 = u^5 \cdot u = u^3+u^2+u = u^2+1,$
$u^7 = u^6 \cdot u = u^3+u = 1$

$G = \{1, u, u^2, u+1, u^2+u, u^2+u+1, u^2+1\}$
$\Rightarrow |G| = 7$

$x = 4$

Ex 7.) $(P, a, y) = (u^3+u+1, u, u^2+u)$
$m = u^2+u+1, \quad k = 3$
Task: find x
$y = a^x \bmod P = u^x \bmod u^3+u+1 = u^2+u$

$u^4 = u^2+u \pmod{u^3+u+1}$

$\underline{\underline{x = 4}}$