Crypto 1 GÜ 9

1.8. Zusatzübung 14:00 Crypto 1
15:30 Crypto 2

8.8. Consultation hour 14:00

Seminarraum T1 @ WSH

HW 9

~~2~~ 1.) Calculate $1031^{-1} \bmod 2227$

Inverse exists, if $\gcd(1031, 2227) = 1$
$\hat{=}$ relatively prime

Use the extended Euclidean algorithm
to calculate $\gcd(a, b) = x \cdot a + y \cdot b$

Use the following scheme for $\gcd(a, b)$, $a > b$

Initialize: $a_2 = r_0 = a$, $b_2 = r_1 = b$
$c_0 = d_1 = 1$, $c_1 = d_0 = 0$

$n = 2$: 1.) Calculate $f_n \in \mathbb{N}$ and $0 \le r_n < b_n$:

$$r_n = a_n - f_n \cdot b_n$$

2.) $c_n = c_{n-2} - f_n \cdot c_{n-1}$

3.) $d_n = d_{n-2} - f_n \cdot d_{n-1}$

4.) $a_{n+1} = b_n$

5.) $b_{n+1} = r_n$

6.) stop, if $r_n = 0$, or goto 1.) with
$n \leftarrow n+1$

n	a_n	b_n	f_n	r_n	c_n	d_n
0				2227	1	0
1				1031	0	1
2	2227	1031	2	165	1	-2
3	1031	165	6	41	-6	13
4	165	41	4	$\boxed{1}$	25	-54
5	41	1	41	0		

$r_0 = c_0 \cdot a + d_0 \cdot b$

$r_1 = c_1 \cdot a + d_1 \cdot b$

$r_2 = 1 \cdot a_2 - 2 \cdot b_2$
$= 1 \cdot r_0 - 2 \cdot r_1$
$= 1 \cdot (1a + 0b) - 2(0 \cdot a + 1 \cdot b)$
$= 1a - 2b$
$= c_2 a - d_2 b$

per Ind.

$\Rightarrow r_n = c_n \cdot a + d_n \cdot b$

$\Rightarrow \gcd(2227, 1031) = 1$

$= 25 \cdot 2227 - 54 \cdot 1031 \equiv 1 \mod 2227$

$\Rightarrow -54 \equiv 2173 \equiv 1031^{-1} \mod 2227$

E30.)

Prove the Chinese Remainder Theorem

$m_1, \dots, m_r$ pairwise relatively prime

$a_1, \dots, a_r \in \mathbb{N}$

$x \equiv a_i \mod m_i \quad i = 1, \dots, r$

has unique solution mod $M = \prod_{i=1}^{r} m_i$ given ~~by~~ $x = \sum_{i=1}^{r} a_i M_i Y_i \mod M$ where

$M_i = M / m_i, \quad Y_i = M_i^{-1} \mod m_i, \quad i = 1, \dots, r$

1.) $x = \sum_{i=1}^{r} a_i M_i y_i \mod M$ is a solution

Let $j \in \{1, \dots, r\}$ $\quad m_j \mid M_i \quad \forall i \neq j$

$\Rightarrow M_i \equiv 0 \mod m_j \quad \forall i \neq j$

$Y_j M_j \equiv 1 \mod m_j$

Crypto1 GÜ 9

$$\Rightarrow x = \sum_{i=1}^{r} a_i M_i y_i \equiv a_j M_j y_j \equiv a_j \mod m_j$$

2.) uniqueness:

Assume 2 solutions y and z exist

$\Rightarrow y \equiv a_i \mod m_i \quad \wedge \quad z \equiv a_i \mod m_i$ $\quad i = 1, \dots, r$

$\Rightarrow y - z \equiv 0 \mod m_i \quad i = 1, \dots, r$

$\Rightarrow m_i \mid y - z \quad i = 1, \dots, r$

$\Rightarrow M \mid y - z$ as $m_1, \dots, m_r$ are pairwise relatively prime

$\Rightarrow y = z \mod M$

E31.) Solve

$x \equiv 3 \mod 11$

$x \equiv 5 \mod 13$

$x \equiv 7 \mod 15$

$x \equiv 9 \mod 17$

$\Rightarrow \underbrace{11, 13, 15, 17}_{m_i}$ pairwise rel. prime

$M = 11 \cdot 13 \cdot 15 \cdot 17 = 36465$

$M_1 = M / 11 = 3315$, $M_2 = M / 13 = 2805$,

$M_3 = M / 15 = 2431$, $M_4 = M / 17 = 2145$

$y_1 = 3315^{-1} \mod 11 \equiv 4^{-1}$ [$3315 = 11 \cdot 300 + 11 + 4$]

$\mod 11 \equiv 3 \mod 11$

$y_2 = 2805^{-1} \mod 13 \equiv 10^{-1} \mod 13$ [$2805 = 13 \cdot 200 + 13 \cdot 15 + 10$]

$\equiv 4 \mod 11$

$y_3 = 2431^{-1} \mod 15 \equiv 1^{-1} \mod 15$ [$2431 = 15 \cdot 100 + 15 \cdot 60 + 15 \cdot 2 + 1$]

$\equiv 1 \mod 15$

$$y_4 = 2145^{-1} \bmod 17 \equiv 3^{-1} \bmod 17 \equiv 6 \bmod 17$$

[...]

$$x = \sum_{i=1}^{r} a_i M_i y_i = 3 \cdot 3315 \cdot 3 + 5 \cdot 2805 \cdot 4$$
$$+ 7 \cdot 2431 \cdot 1 + 9 \cdot 2145 \cdot 6$$
$$= 218782 \equiv 36457 \bmod M = 36465$$