Crypto 1 Ü3

28. APR. 2011

8.) $\pi = (1)(2,11,5,8)(3,6,7,4)(9,10)$

$$\Rightarrow \pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 1 & 11 & 6 & 3 & 8 & 7 & 4 & 2 & 10 & 9 & 5 \end{pmatrix}$$

Message space of a finite sequence of length $k=11$

$$\mathcal{M} = \{(m_1, \dots, m_{11}) \mid m_i \in \mathcal{X}\}$$

with alphabet $\mathcal{X} = \{a, b, \dots, z\} = \{0, 1, \dots, 25\}$

$|\mathcal{X}| = 26$

a.) There are blocks where the permutation is cyclic.

$\Rightarrow$ These blocks are not changed if each letter inside one block is equal.

$$\Rightarrow \hat{\mathcal{M}} = \{(m_1, \dots, m_{11}) \mid m_1 \in \mathcal{X},\ m_2 = m_{11} = m_5 = m_8 \in \mathcal{X},\ m_3 = m_6 = m_7 = m_4 \in \mathcal{X},\ m_9 = m_{10} \in \mathcal{X}\}$$

$\Rightarrow$ number of sequences

$|\hat{\mathcal{M}}| = |\mathcal{X}| \cdot |\mathcal{X}| \cdot |\mathcal{X}| \cdot |\mathcal{X}| = |\mathcal{X}|^4 = 456976$ (✓)

compound to $|\mathcal{M}| = |\mathcal{X}|^{11} = 3{,}6 \cdot 10^{15}$

an unchanged plaintext in english: Mississippi

9.) Number theory of the gcd

a.) Prove that $a \in \mathbb{Z}_m$ invertible
$\Leftrightarrow \gcd(a,m)=1$

$\gcd(a,b) = a \cdot x + b \cdot y$

$\Rightarrow 1 = \gcd(a,m) \cdot \Leftrightarrow ax + my = 1$
(given in hint)

$\Rightarrow ax - 1 = -my$
$\Leftrightarrow m \mid (ax-1)$
$\Leftrightarrow ax \equiv 1 \pmod m$ $\quad (ax = 1)$ definition of the inverse element
$\Leftrightarrow x \equiv a^{-1} \pmod m$ □

b.) prove that: $\gcd(a,b) = \gcd(b,r)$ with given constraints

$d := \gcd(a,b) \Rightarrow d \mid a$ and $d \mid b$
$\Rightarrow d \mid (ax+by)$
↑ iff 1 Ex 3c

$\Rightarrow d \mid \underbrace{(a-bq)}_{r}$ $\Rightarrow d \mid r \Rightarrow d \mid r$ and $d \mid b$
$\exists\, r = a - bq$
$\Rightarrow \gcd(r,b) = d$
$\Rightarrow \gcd(b,r)$ □

Crypto 1 ü 3

28. APR. 2011

c.) def $c = a \cdot b$. With the condition $\gcd(a,b)=1$ we achieve that $\{a, b, 1\}$ are the only divisors of c

$\Rightarrow \gcd(c,m) = \gcd(a \cdot b, m) = \gcd(a,m) \cdot \gcd(b,m)$ □

Remark: $\gcd(a,b)$ is sufficient but not necessary

e.g. for $a = b = 2$, $m = 4 \Rightarrow \gcd(a,b) = 2 \neq 1$

$\gcd(c,m) = 4 = \gcd(a,m)\gcd(b,m)$

d.) Properties of a multiplicative group ($\gcd(a, b, c \in \mathbb{Z}_m^*)$)

- closure: since $\gcd(a,b)=1$ and $\gcd(a,m)=\gcd(b,m)=1$ $\overset{(c.)}{\Rightarrow} \gcd(a \cdot b, m) = 1$ (Product is still an element of the group)
- commutativity: $\gcd(a \cdot b, m) = \gcd(b \cdot a, m)$
- associativity: $\gcd(a \cdot \gcd(b \cdot c, m), m)$

$\overset{(c.)}{=} \gcd(a \cdot \gcd(b,m) \cdot \gcd(c,m), m)$

$= \gcd(\gcd(a, b, m) \cdot c, m)$

- neutral element: $1 \cdot a = a \cdot 1 = a$ and $a, 1 \in \mathbb{Z}_m^*$
- inverse element: for all $a \in \mathbb{Z}_m^*$ $a^{-1} \in \mathbb{Z}_m^*$ since $\gcd(a,m)=1$ (a is in (a))

$\Rightarrow \mathbb{Z}_m^*$ is a multiplicative group □

e.) $\exists\, 221^{-1} \in \mathbb{Z}_{2310}$?

$\Rightarrow \gcd(2310, 221) = 1$

(use (b.) iteratively:
(Euklidean algorithm (EA))
($\gcd(bq+r, b) = \gcd(r, b)$)

$2310 = 221 \cdot 10 + 100$
$a \quad b \quad q \quad r$

$221 = 100 \cdot 2 + 21$

$100 = 21 \cdot 4 + 16$

$21 = 16 \cdot 1 + 5$

$16 = 5 \cdot 3 + 1$ $\Rightarrow \gcd(2310, 221) = 1$

$\Rightarrow 221^{-1} \in \mathbb{Z}_{2310}$ □

10.)

a.)

i		K_i	P_i
0	a	1	0
1	b	4	6
2	c	12	66
3	d	4	6
4	e	2	1
5	f	1	0
6	g	6	15
7	h	2	1
8	i	7	21
9	j	2	1
10	k	14	91
11	l	7	21
12	m	1	0
13	n	3	3
14	o	4	6
15	p	4	6
16	q	4	6
17	r	10	45
18	s	4	6
19	t	0	0
20	u	0	0
21	v	9	36
22	w	6	15
23	x	8	28
24	y	3	3
25	z	0	0

$K_i \hat{=}$ total appearances of letter i;

$P_i \hat{=}$ number ordered pairs $\binom{K_i}{2}$

Crypto 1 ü 3

28. APR. 2011

$n = 14 \cdot 8 + 6 = 118$

bin coefficient $\binom{n}{2} = \frac{n!}{(n-2)!\,2!} = \frac{n(n-1)}{2} = 6903$

$$I_c = \frac{|\{(i,j) \mid c_i = c_j,\ 1 \le i < j \le n\}|}{\binom{n}{2}} = \frac{\sum_{i=0}^{25} \binom{k_i}{2}}{\binom{n}{2}}$$

$$= \frac{6 \cdot 0 + 3 \cdot 1 + 2 \cdot 3 + 6 \cdot 6 + 2 \cdot 15 + 2 \cdot 21 + 1 \cdot 28 + 1 \cdot 36 \ldots}{\ldots + 1 \cdot 45 + 1 \cdot 66 + 1 \cdot 91}{6903}$$

$$= \frac{383}{6903} \approx 0{,}055483$$

$\Rightarrow$ This text is mono-alphabetic and
English ($I_c = 0{,}0668$)
polyalphabetic ($I_c = 0{,}0585$)

Vigenere cipher:

„All the world is a stage, and all the men and women merely players: They have their exits and their entrances, and one man in his time plays many parts, "

Act 2, Scene 7 blabla Shakespeare

Key: kee