05. MAI 2011

Crypto 1 ü 4

In Appendix A a group is defined as a set G with

(i) $(a \circ b) \circ c = a \circ (b \circ c) \quad \forall a, b, c \in G$

(ii) $\exists e \in G : a \circ e = e \circ a = a \quad \forall a \in G$

(iii) $\forall a \in G \quad \exists a' \in G : a \circ a' = a' \circ a = e$

Ex 9 a.)

$gcd(a, m) = gcd(b, m) = 1$

$\Rightarrow gcd(a \cdot b, m) = 1$

Ex 11.)

$G = \{ A \mid A \in K^{n \times n} \text{ regular} \}$

It holds $(A \cdot B)_{ij} = \sum_{k=1}^{n} a_{ik} \cdot b_{kj} \quad (*)$

(i) $((A \cdot B) \cdot C)_{ij} \overset{(*)}{=} \sum_{k=1}^{n} (A \cdot B)_{ik} \cdot c_{kj}$

$$\overset{(*)}{=} \sum_{k=1}^{n} \sum_{l=1}^{n} a_{il} b_{lk} c_{kj}$$

$$= \sum_{l=1}^{n} a_{il} \sum_{k=1}^{n} b_{lk} c_{kj} \overset{(*)}{=} \sum_{l=1}^{n} a_{il} (B \cdot C)_{lj}$$

$$\overset{(*)}{=} (A \cdot (B \cdot C))_{ij}$$

(ii) $E_n = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & \ddots & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix} \Rightarrow \forall A \in G : A \cdot E_n = E_n \cdot A = A$

(iii) As G contains only regular matrices by def., it holds

$\forall A \in G \; \exists A^{-1} \in G : A \cdot A^{-1} = A^{-1} \cdot A = E_n$

$\Rightarrow$ G is a multiplicative group.

G is an abelian group

$\Leftrightarrow \forall A, B \in G : A \cdot B = B \cdot A$

It is an abelian group for $n = 1$

otherwise, e.g. $K = \mathbb{R}$, $n = 2$, $a \neq 1$, $a \neq 0$

$A = \begin{pmatrix} 0 & 1 \\ a & 0 \end{pmatrix}$ $B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ with $A^{-1} = \begin{pmatrix} 0 & 1/a \\ 1 & 0 \end{pmatrix}$

$B^{-1} = B$

$\Rightarrow A, B \in G$

$\Rightarrow A \cdot B = \begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix}$ / $B \cdot A = \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$

$\Rightarrow A \cdot B \neq B \cdot A$

$\Rightarrow$ G is <u>not</u> in general abelian.

<u>Ex 12)</u>

<u>a.)</u> It is $c_i = \begin{cases} m_i + k_i \pmod{26} & 0 \leq i \leq n-1 \\ m_i + c_{i-n} \pmod{26} & n \leq i \leq l-1 \end{cases}$

$c_n = m_n + c_0 \Leftrightarrow m_n = c_n - c_0 \pmod{26}$

$c_{n+k} = m_{n+k} + c_k \Leftrightarrow m_{n+k} = c_{n+k} - c_k \pmod{26} \quad k \in \mathbb{N}_0$

Try $n = 1, 2, \ldots$

Problems: - $m_0, \ldots, m_{n-1}$

- How to determine n?

05. MAI 2011

Crypto 1 Ü4

b.) 3 11 6 21
D L G V
D L G
n=1: –
I V P No, it's not n=1

n=2: D L G V T
D L G
–
D K N No, it's not n=2

n=3: D L G V T Y O A C O U V C E Z A
–{K E Y}D L G V T Y O A C O U V C
{T H I}S I S T H E A U T O K E Y

"D L G" – "T H I" = "K E Y"

(c.) $c_i = \begin{cases} m_i + k_i \pmod{26} & 0 \le i \le n-1 \\ m_i + m_{i-n} \pmod{26} & n \le i \le l-1 \end{cases}$

If I have the character of the message and if I know n, then I can calculate every n-th character!
e.g.: I know $m_k \Rightarrow m_{k+n} = c_{k+n} - m_k \pmod{26}$
it follows: I need to guess m_k!
Try a Friedmann attack, e.g. 'e' + 'e' = 'i',
i.e. if $c_i = i$ there is a relative high ~~chance~~ probability that m_i and m_{i-n} are 'e'.

d.) c = Q E X Y I R V E S I U X K Q V F C H K G $m_i = c_i - m_{i-n}$
T H E R A E B E T E M T O D S $m_{i-n} = c_i - m_i \pmod{26}$

Ex 13.) We are following the Kasiski-Babbage-Method, which exploits the behaviour of

$$V_{ij} = \begin{cases} 1 & \text{if } c_i = c_q \\ 0 & \text{otherwise} \end{cases}$$

then $E[Y_{ij}] = \begin{cases} \kappa_u & \text{if } i \sim j \quad (i-j \equiv 0 \bmod k) \\ \frac{1}{m} & \text{otherwise } \left[P(k_i = l) = \frac{1}{m}\right] \end{cases}$

It follows for $m = 26$ with textlength u and $\kappa_u = \kappa_e = 0,066895$

$$k \approx \frac{0,028437 \cdot u}{(u-1) l_c - 0,0385\, u + 0,066895}$$

$$E(I_c) = \frac{1}{u(u-1)} \sum_{i=0}^{m-1} n_i (n_i - 1) = l_c \approx 0,04304$$

First guess $k \approx 6,25643 \Rightarrow k = 6$

Calculating maximum frequency of $c = (c_0, c_6, c_{12}, \ldots, c_{356})$

reveals: x: 6,39 % << 12,51 % (frequency of e in natural language)

next $k = 7$: reveals max. freq. of letters are $\leq$ 7,86 %

$k = 5$: -"- is $\approx$ 14,4 %