

ÜBCHI

Jako hlavní německý polní šifrový systém za I.světové války (především na francouzsko-německé frontě) byla používána šifra ÜBCHI. Skládala se z dvojité sloupcové (neúplné) transpozice vylepšené o vložení několika klamačů mezi první a druhou transformací. Počet klamačů byl určen počtem slov klíčové fráze. Francouzi šifru byli schopni luštit. Pomáhalo jim především využití tzv. předpokládaných slov. Tedy slov, které se v otevřeném textu vyskytovaly. Tato slova měly luštitelé k dispozici zejména díky stereotypnosti německých hlášení. Metoda, která je založena na znalosti slova v otevřeném textu je pro případe transpozičních šifer velmi účinná (blíže viz Luštění se znalostí otevřeného textu (Know-plaintext attack)).

Příklad – postup při šifrování pomocí šifrového systému ÜBCHI

Nejprve zvolíme heslo a provedeme jeho permutační vyčíslení :

```
C T E N A R O K A
3 9 4 6 1 8 7 5 2
```

(vyčíslení se provádí přiřazením čísel jednotlivým písmenům, čísla se přiřazují v abecedním pořádku, pokud se nějaké písmeno opakuje je nižší hodnota přiřazena jeho prvnímu výskytu v klíči)

Klíče v originální šifře bývaly dlouhé přes dvacet znaků. Klíč a jeho permutační vyčíslení určuje velikost transpoziční tabulky (v našem případě to bude 9 sloupců) a počet klamačů, které se přidají na konec první transpozice (v našem případě dva, neboť klíč je tvořen dvěma slovy). Šifra lze zkomplikovat, pokud budeme používat v prvním a druhém kroku odlišné permutační heslo. Originální šifra ÜBCHI (tak jako v našem případě) však často používala pouze heslo jedno.

Nyní si připravíme otevřený text (přepsaný do mezinárodní abecedy) :

KDYZ MI NECO VYSVETLIS ZAPOMENU TO KDYZ TO ALE SAM UDELAM
POCHOPIM TO

První transpozice se vytvoří tak, že zpráva se nejprve vepíše pod klíčovou frázi po řádcích

```
C T E N A R O K A
3 9 4 6 1 8 7 5 2
K D Y Z M I N E C
O V Y S V E T L I
S Z A P O M E N U
T O K D Y Z T O A
L E S A M U D E L
A M P O C H O P I
M T O
```

Potom se vepisuje zpráva znovu pod klíč. Jednotlivé sloupky předchozí tabulky se vepisují po řádcích a to v pořadí permutačního vyjádření

```
3 9 4 6 1 8 7 5 2
M V O Y M C C I U
A L I K O S T L A
M Y Y A K S P O E
L N O E P Z S P D
A O N T E T D O I
```

E M Z U H D V Z O
E M T A E

Na závěr se přidají dvě písmena – klamače (označeny červeně). Dvě, protože klíčová fráze má dvě slova. Jejich hodnota může být libovolná, ale neměly by to být např. písmena X Q nebo jiná málo četná písmena. Taková písmena by luštitelům naopak pomohla určit velikost tabulky a možné umístění dvou sloupců. Proto jsou v našem příkladě jako klamače uvedena písmena A a E.

Šifrový text se získá vypsáním sloupců této tabulky do jednoho řádku. Sloupky se opět vypisují v pořadí permutačního vyjádření.

M O K P E H E U A E D I O M A M L A E E O I Y O N Z T I L O P
O Z Y K A E T U A C T P S D V C S S Z T D V L Y N O M M

Výsledný šifrový text se získá rozdělením do skupin po pěti znacích.

MOKPE HEUA E DIOMA MLAE E OIYON ZTILO POZYK AETUA CTPSD VCSSZ
TDVLY NOMM

Abyste mohli lépe sledovat, jak se jednotlivé znaky postupně vepisují do tabulek a případně, jak probíhá jejich promíchání během přípravy šifrového text, označili jsme vybraná písmena následovně :

fialově - prvních devět písmen otevřeného textu

modře – písmena ve sloupci, který vstupuje do první transpozice jako první

červeně – klamače přidáné po první transpozici

hnědě – písmeno, které patří mezi prvních devět písmen otevřeného textu a současně leží ve sloupcu, který jako první vstupuje do transpoziční tabulky