

Kryptografins grunder: hemtal 1

Erik Tjernlund*

750519-0137

d98-etj

6 maj 2002

1 Geheimschreiber

2 Vigenérechiffer

Uppgiften var att få tag i klartexten till en text som blivit krypterat med ett okänt chiffer. Misstänkte snabbt att ett vigenérechiffer använts, bland annat på grund av att bokstavsfrekvenserna var relativt jämnt fördelade.

2.1 Hitta nyckellängden

Försökte först hitta nyckellängden genom att gissa en längd och sedan beräkna *The Index of Coincidence*. Skrev ett program i perl som beräknade detta och fann nyckellängden troligen var 21 tecken lång.

2.2 Hitta nyckelordet

Man kan hitta nyckelordet (när man har en god gissning på längden) genom att för varje nyckelposition, beräkna *The Mutual Index of Coincidence* för varje bokstav i alfabetet. Skrev ett perlprogram som gjorde detta och fann direkt ordet PERMUTATIONSVIDDJTJUGO. Hurra!

2.3 Dekryptering

Dekryptering är enkelt eftersom det bara är att dra differensen av kryptotexten och nyckelordet i modulo 26 (tvärtemot krypteringen). Tyvärr fann jag att jag ropat "Hurra!" för tidigt. Den förväntade klartexten kom inte fram, bara mer kryptotext.

Kom till slutsatsen, med hjälp av nyckelordet, att varje 20 teckens substräng av klartexten blivit omkastad, likt kolumner i en matris.

*I samarbete med Emanuel Viklund (d98-evi)

2.4 Permuteringen

För att hitta hur tecknen i substrängarna (med 20 tecken i varje) var omkastade, försökte jag först skriva ett program som tog en substräng som innehöll ett T och ett H — TH är det vanligaste bigrammet i engelskan — och sedan tittade på de permuteringar som uppstod i resten av texten då jag passade in TH på olika platser i substrängen.

Tanken var alltså att mäta statistik på de bigram en sådan permutering skulle ge uppskov till i resten av texten. Detta fungerade halvbra, men efter en del problem insåg jag att en lite mer ”low tech” variant var snabbare och enklare.

Skrev helt enkelt ut ett antal rader av den permuterade texten och radbröt den efter 20 tecken.

```
WSILIETSVDRENAAOUECN
WIEDDLPACDEHANNNTRRO
SIEHCALBTIAHOBTAELRE
AEEVRTWUSENINRDNODNL
MTYBHERWC SLARIDIOLLE
TEELDNCIFMUULULIRMNI
CRANCDEUACENRNOHSACH
TBT PBRHIWORNTDAHEAEI
IEELAITNABTCKKOCOHLL
```

Klippte isär varje utskrivna kolumn och försökte pussla ihop dem i en ny ordning. Beväpnad med det faktum att i engelskan följs alltid ett Q av ett U och att det vanligaste trigrammet är THE, gick det ganska fort att hitta permuteringen. Texten visade sig vara Lewis Carolls *Alice in wonderland*:

```
ALICESADVENTURESINWONDERLANDCHAPTERIDOWNTHERABBITHOLEALICES
ADVENTURESINWONDERLANDBYLEWISCARROLLTHEMILLENNIUMFULCRUMEDI
TIONACDUNCANRESEARCHCHAPTERIDOWNTHERABBITHOLELINKBACKTOTHEA
LICE...
```

3 AES

Skrev en implementation av AES. Hastigheten verkar ligga runt 490-500 kbyte/sekund. Skickad till migo@nada.kth.se.

4 Slumptalsgeneratorer

5 DES och S-Boxarna

6 Mer DES

7 Irreducibelt polynom

Med hjälp av *Handbook of Applied Cryptography* hittade jag ett irreducibelt polynom av grad 5 som genererar kroppen $GF(2^5)$:

$$x^5 + x^2 + 1$$

Elementen i kroppen blir då:

$0 = 0$	$a^7 = a^2 + a^4$	$a^{15} = 1 + a + a^2 + a^3 + a^4$	$a^{23} = 1 + a + a^2 + a^3$
$a^0 = 1$	$a^8 = 1 + a^2 + a^3$	$a^{16} = 1 + a + a^3 + a^4$	$a^{24} = a + a^2 + a^3 + a^4$
$a^1 = a$	$a^9 = a + a^3 + a^4$	$a^{17} = 1 + a + a^4$	$a^{25} = 1 + a^3 + a^4$
$a^2 = a^2$	$a^{10} = 1 + a^4$	$a^{18} = 1 + a$	$a^{26} = 1 + a + a^2 + a^4$
$a^3 = a^3$	$a^{11} = 1 + a + a^2$	$a^{19} = a + a^2$	$a^{27} = 1 + a + a^3$
$a^4 = a^4$	$a^{12} = a + a^2 + a^3$	$a^{20} = a^2 + a^3$	$a^{28} = a + a^2 + a^4$
$a^5 = 1 + a^2$	$a^{13} = a^2 + a^3 + a^4$	$a^{21} = a^3 + a^4$	$a^{29} = 1 + a^3$
$a^6 = a + a^3$	$a^{14} = 1 + a^2 + a^3 + a^4$	$a^{22} = 1 + a^2 + a^4$	$a^{30} = a + a^4$

Enligt uppgiften ska jag nu beräkna $\alpha\beta$ där α ges av polynomet $a^4 + a + 1 = a^{17}$ och β är alla elementen i kroppen:

$$\begin{aligned} 0 \cdot a^{17} &= 0 \\ a^0 \cdot a^{17} &= a^{17} \\ a^1 \cdot a^{17} &= a^{18} \\ a^2 \cdot a^{17} &= a^{19} \\ &\vdots \\ a^{13} \cdot a^{17} &= a^{30} \\ a^{14} \cdot a^{17} &= a^0 \\ a^{15} \cdot a^{17} &= a^1 \\ &\vdots \\ a^{30} \cdot a^{17} &= a^{16} \end{aligned}$$