Fakulteta za matematiko in fiziko
Fakulteta za računalništvo in informatiko

ARNE BEURLING IN G-SCHREIBER V DRUGI SVETOVNI VOJNI

Izdelal:
Leonard Štefančič

Ljubljana,Junij 2012

Povzetek

Arne Beurling je v svojem času bil veliko ime tako na področju matematike kot kriptografije. Ta prispevek opisuje njegovo kriptografsko delo, ki predstavlja velik prispevek k strokovnem razvoju ne samo švedske, temveč tudi svetovne kriptografije.

Še več, le v dveh tednih mu je uspelo razbiti nemški G-Schreiber algoritem, kar je neverjeten uspeh upoštevaje kompleksnost tega algoritma. V tem prispevku je opisana Beurlingova analiza za razbitje G-Schreiberjeva algoritma. To mu je uspelo kljub dejstvu, da ni imel konkretnega znanja o delovanju takratnih teleprinterjev. Podani so tudi principi delovanja G-Schreiberjeve naprave, ki so nujni za razumevanje Beurlingovega dela.

Abstract

During his time Arne Beurling was not only an important name in the field of mathematics but also one of the leading men in the field of cryptography. This paper briefly describes his enormous quintessential contribution to Swedish cryptography as well as the development and importance of cryptography throughout the world.

Moreover Beurling was able to decipher German G–Schreiber algorithm in the period of two weeks. Knowing the complexity of the G-Schreiber algorithm, it is hard to believe that it could be broken barely in two weeks. Especially given the fact that when Beurling started to work on the problem, he knew nothing about teleprinters, never mind teleprinter ciphering.This paper describes Beurling's analysis for the deciphering of the G Schreiber algorithm and basic principles of G Schreiber machine.

Kazalo

1 Uvod

V tem prispevku so opisane razmere in razlogi, ki so botrovali enemu naj bolj pomembnih dogodkov v zgodovini kriptografije, ko je švedski matematik Arne Beurling dešifriral nemško kodo znano kot G-Schreiber. Za potrebe analize tega procesa je v nadaljevanju predstavljeno funkcioniranje naprave znane pod imenom G-Schreiber. Nemci so napravo in kodo uporabljali za strateško komuniciranje že pred 2. svetovno vojno. Danes je znano, da je dešifriranje G-Schreiberjeve kode bil pomemben strokoven uspeh švedske kriptografije. Poleg tega je to dešifriranje imelo strateški pomen, ker je pripomoglo k pridobivanju pomembnih informacij, še posebej tistih v zvezi s tajno operacijo Barbarossa.

Švedski državi je v tem času veliko nevarnost, poleg nacistične Nemčije, predstavljala Sovjetska Zveza. Zaradi obvladovanja teh rizikov so Švedi leta 1937 ustanovili DSHQ (Defense Staff Headquarters). Znotraj DSHQ je bil organiziran kripto oddelek, ki ga je vodil Eskil Gester. Leta 1939 je Gester vključil Beurlinga v delo ruske sekcije DSHQ. V tem času je to bila najbolj pomembna sekcija DSHQ. Tako je bil Beurling neposredno vključen v delo na področju razbitja tim. ruske 4-mestne in 5-mestne šifre, ki jo je ruska mornarica uporabljala na Baltskem morju.

V prispevku so navedeni pomembnejši dogodki in principi delovanja Arnie Beurlinga. Pozornost je posvečena predvsem znanim podrobnostim iz njegovih uspešnih kriptoanaliz.

S pomočjo analize Beurlingovega dela na področju razbitja nekaterih klasičnih kriptosistemov smo hoteli pokazati potek razbitja teh kod v praksi. V seminarski nalogi smo podrobneje opisali postopke razbitja kriptosistema G-Schreiberjeve kode.

Delno smo pokazali tudi razloge in praktičen potek za načrtovanja sistemov kriptografije, ki so ga oblikovali nemški kriptografi.

Z analizami razbitja teh sistemov smo želeli poudariti tudi pomen vzdrževanja visokega nivoja zaščite varnosti kriptografskih sistemov.

Vsebina prispevka je organizirana v 5.poglavjih. Bistvene strokovne vsebine pa so opisane predvsem v spodaj navedenih poglavjih:

- V 2.poglavju je predstavljeno funkcioniranje teleprinterja kot mehanske naprave, ki se je v 20.stoletju lahko uporabljala tudi za potrebe šifriranja.

– V 3.poglavju je opisana originalna verzija elektromehanske naprave z imenom G-Schreiber, ki se je uporabljala za prenašanje velikega števila skrivnih poročil preko telegrafskih inštalacij. Tovrstne naprave so kriptografom omogočale oblikovanje kompleksnih kriptografskih sistemov. Tako so nemški kriptografi oblikovali G-Schreiberjevo kodo. Algoritem in način prenašanja podatkov s pomočjo G-Schreiberjeve naprave je opisano v drugem delu 4.poglavja.

– V 4.poglavju je podana rekonstrukcija možnega poteka Beurlingovega dela na področju razbitja G-Schreiberjevega algoritma. Gre za analizo sistema dekodiranja, ki ga tudi danes občudujemo. Genialnost Beurlingovega sistema je toliko večja, ko se zavemo, kako malo časa in malo tehničnih pripomočkov je potreboval za razbitje te kompleksne kode.

2 Teleprinter

V tem poglavju so podani osnovni tehnični principi delovanja teleprinterskih naprav in standardi pri prenosu tekstov

2.1 Opis naprave

Prvi teleprinterji so se pojavili konec 19 stoletja. Glavni namen teh naprav je bil nadomeščanje Morsejeve telegrafije z novim sistemom, ki omogoča avtomatski sprejem teksta, natipkanega na (lahko tudi zelo oddaljeni) tipkovnici oddajnika. Tekst, natipkan na oddajniku teleprinterja, se pošilja do sprejemne točke in potem tiska popolnoma avtomatsko, brez kakršnekoli človeške intervencije.

Vsak znak, ki se pošilja s teleprinterjev, predstavlja zaporedje petih impulzov. Obstajata dve vrsti impulzov in sicer pozitivni in negativni. Impulzi so predstavljeni kot dve vrsti: negativni "0" bodisi kot "1". Obe vrsti impulzov imata enako dolžino. Ta značilnost teleprinterskih znakov se bistveno razlikuje v primerjavi z Morsejevim sistemom.

Pritisk na teleprintersko oddajno tipkovnico generira stanje bodisi s tokom ali stanje brez toka. Ta stanja se kreirajo v petih vzporednih poteh (linijah). Komutator v urejenem vrstnem redu prebere vseh pet linij. Potem ustvari impulze '0' ali '1' ter te impulze pošilja po "linijah". Na sprejemnem mestu podoben komutator interpretira impulze in ustvarja vzorce, ki sestavljajo stanje tok ali brez toka. S tem kontrolira mehanizem pisalnega stroja, ki tako natisne pravilen znak.

Obstaja tudi alternativna uporaba teleprinterja glede na zgoraj opisano. Pri tej gre za tipkanje sporočila direktno na linijo. V tem primeru se na papirnem traku z luknjanjem ustvarjajo vzorci luknje/brez lukenj, kar odgovarja vzorcem elektrika je/elektrike ni. Pri pošiljanju sporočila se papirnati trak vstavi v napravo, ki je fiksirana v teleprinterju. Ta naprava opravlja funkcijo branja, interpretiranja in prenašanja znakov. Na sprejemni točki lahko sporočilo pridobimo na tri načina:

1. neposredno tiskanje;
2. papirnati trak se ponovno preluknja za kasnejše tiskanje;
3. izvedba obeh zgoraj navedenih funkcij.

Vzorci na papirnem traku so zelo poučni kadar se opisujejo teleprinterski znaki. Vzorec "luknje/ne luknje" se lahko prezentira kot "1" in "0" ter tako uporablja za moderno izražanje.

S 5-bitno kombinacijo lahko predstavimo le 32 znakov. Glede na dejstvo, da obstaja:

- 26 črk;
- števila od 0 do 9 ter
- tudi določeno število znakov za ločila, znakov za prekinjanje, poudarjanje in naglašanje govora,

je vsekakor za uporabnost teleprinterja koristno najti način povečanja števila znakov. Ista 5-bitna kombinacija lahko predstavlja dva različna znaka, kar je odvisno od uporabljenega nadzornega znaka. Nadzorni znak je lahko označen z LS (Letter Shift – črkovni zamik) ali FS (Figure Shift – zamik figure). LS ali FS morata biti predstavljena takoj pred predstavitvijo samega znaka. Ko se pojavi LS, se vsi naslednji znaki interpretirajo kot LS označbe do pojava FS označbe in tako naprej.

Letter shift	*Order of pulses* 12345	*Figure shift*	*Swedish notation*
A	11000	–	
B	10011	?	
C	01110	:	
D	10010	*"Who's there?"*	
E	10000	3	
F	10110	*CS*	
G	01011	*CS*	
H	00101	*CS*	
I	01100	8	
J	11010	*Bell*	
K	11110	(	
L	01001	)	
M	00111	.	
N	00110	,	
O	00011	9	
P	01101	0	
Q	11101	1	
R	01010	4	
S	10100	'	
T	00001	5	
U	11100	7	
V	01111	=	
W	11001	2	
X	10111	/	
Y	10101	6	
Z	10001	+	
CR	00010	*CR*	1
NL	01000	*NL*	2
LS	11111	*LS*	3
FS	11011	*FS*	4
SP	00100	*SP*	5
BL	00000	*BL*	6

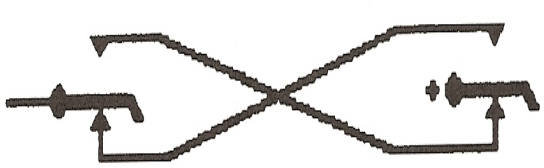
Slika 1: Mednarodni teleprinterski kodni zapis CCITT2

2.2 Uporaba teleprinterja za potrebe šifriranja

Pri pošiljanju šifriranega sporočila se velikokrat izgubi pomen razlike med LS stanjem in FS stanjem. Glede na dejstvo, da luknjičaste označbe lahko nosijo kompletno informacijo, je švedska kriptografska agencija nadomestila znake, ki so neprimerni za tiskanje, s številkami 1-6, kar je prikazano tudi v prejšnji tabeli.

Ključ znakov, ki ga je vseboval papirnati trak je lahko bil oblikovan v dveh kopijah, kar pomeni da je vsaka stran povezave imela svojo kopijo. Za pošiljanje sporočila so uporabljali dva čitalnika, enega za ključ, drugega za besedilo. Impulzi oziroma biti, ki so nastajali v čitalnikih so bili nato sešteti v modulu dva (XOR-u) ter se nato rezultati prenašali do sprejemne točke. Impulzi oziroma biti, ki so prispeli do sprejemne točke, so bili rezultat dešifriranja sporočila, njegovega interpretiranja kot telex kode in nazadnje njegovega tiskanja.

Seštevanje z modulom dva (XOR-ing) se lahko izvaja z priredbo enostavne povezave dveh ročajev, ki registrirajo **obstoj ali ne obstoj** lukenj na papirnatih trakovih. Ta povezava je prikazana na spodnji sliki:



Slika 2: mehanski princip XOR

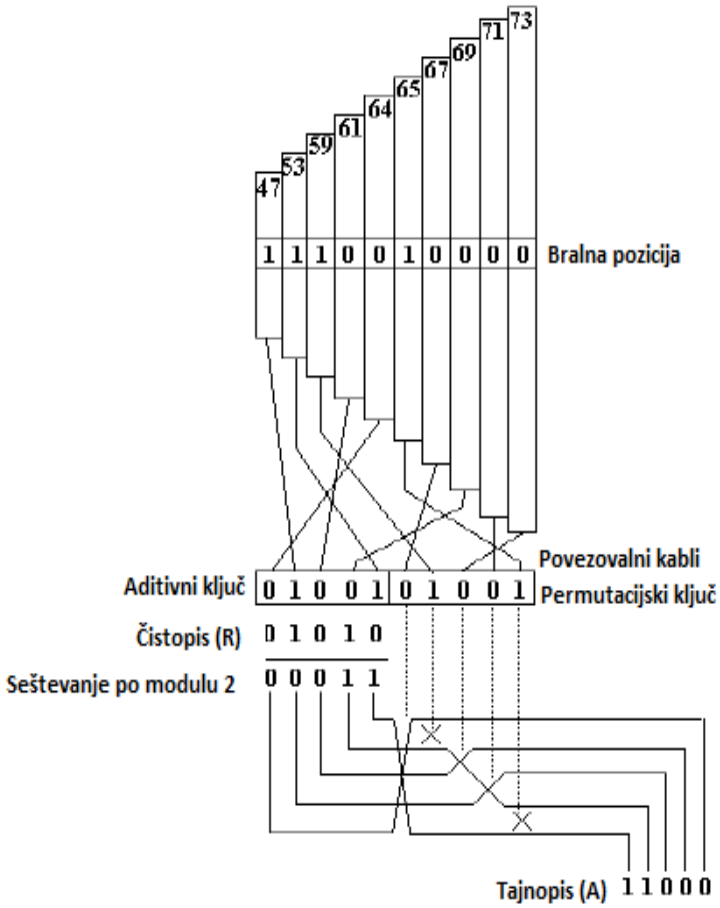
V kolikor "1" pomeni luknja in "0" luknje ni je sistem za povezavo z modulom dva: **0+0= 0; 0+1=1; 1+0=1; 1+ 1=0**. Smisel zgoraj navedene povezave je sledeča tok se kreira ko luknje ni, vendar se stanje brez elektrike pošilja naprej le ko ni luknje ali pa ko sta dve luknji. Za vsak znak je potrebnih pet povezav z modulom dva. Vsaka teh povezava je lahko paralelna ali serijska.

3 G-Schreiberjev algoritem

To poglavje je posvečeno predstavitvi klasične šifre znane pod imenom G-Schreiberjev algoritem, ki so jo Nemci uporabljali za zaščito tajnih sporočil tekom druge svetovne vojne. Vsebina poglavja se začne s predstavitvijo zgodovinskega konteksta uporabe te klasične šifre. Nadaljuje z opisom naprave, ki je omogočala razvoj in učinkovito uporabo šifre. Bistveni vsebinski del poglavja pa je posvečen opisu šifrirnega algoritma. Gre za primer transpozicijske šifre, ki se je uporabljala v klasični kriptografiji. Črke originalnega sporočila ostanejo nespremenjene, njihova mesta pa so pomešana na določen sistematičen način.

V obdobju od 1929 do 1932 je nemška **firma Siemens & Halske** razvila originalno verzijo tim. **Geheimschreiber**-ja. Naprava je bila patentirana pod imenom **Anordnung zur Nachrichtenübermittlung in Geheimschrift über Telegraphenanlagen**. Šlo je za napravo, ki je prenašala skrita sporočila preko telegrafskih inštalacij. V drugi svetovni vojni je imela široko področje uporabe. Uporabljali so jo tako za vojaške namene kot tudi pri diplomatski korespondenci. Iz izvirne naprave so razvili različne modele. Na samem začetku so največ uporabljali model **T52a/b**. Vsi modeli so bili kvalitetno izdelani in zato zanesljivi. To potrjuje dejstvo, da je norveška policija tudi po končani drugi svetovni vojni za pošiljanje skrivnih sporočil še naprej uporabljala vse zajete G-Schreiber-je. Res je, da jih je po vojni bilo potrebno prenoviti, vendar dolgotrajno funkcioniranje teh naprav le kaže na njihovo kakovostno izdelavo.

Za predstavitev poteka Beurling-ove analize je koristno bolj detajlno predstaviti prej omenjeni model T52. Model T52 je elektromehanska naprava z desetimi bakelitnimi kolesi. Vsako kolo posebej ima enako razporejeno število pozicij okoli roba oziroma okoli obroča. Vsaka pozicija je predstavljala vrednost 0 ali pa 1. Prvo kolo je imelo 47 pozicij, ki so bile označene 00-46; drugo kolo je imelo 53 pozicij označene z 00-52; tretje kolo 59 pozicij, naslednje 61,64,65,67,69,71 in zadnje kolo pa je imelo 73 pozicij. Kabli so povezovali kolesa in preostali del stroja. Povezovalne kable je bilo možno poljubno menjavati. V praksi se je vršila menjava kablov v presledku tri do devet dni.



Slika 3: Šifriranje pri G-Schreiberju

3.1 Opis G-Schreiberjevega algoritma

G-Schreiber ima 10 različnih koles, vsako kolo je različne velikosti.

w_{ij}...kolo tipa i položaja j, $w_{ij} \in \{0,1\}$ oz. w_{ij} pripada bit 0 ali bit 1.

1.kolo ima 47 polozajev $w_{1,1}, w_{1,2}, ..., w_{1,47}$
2.kolo ima 53 polozajev $w_{2,1}, w_{2,2}, ..., w_{2,53}$
$\vdots$
10.kolo ima 73 polozajev $w_{10,1}, w_{10,2}, ..., w_{10,73}$.

G-Schreiber ima dva ključa: k_1 za šifriranje 5-bitnih telegrafskih kod ter drugi k_2 za permutacijo že šifriranih 5-bitnih kod.

k_1... aditivni (zamenjalni) ključ
k_2... permutacijski ključ

Izvedba obeh ključev poteka preko povezovalnih kablov med kolesi in posredniki (električnimi releji)

Aditivni ključ je 5-bitni ključ:
$k_1 = a_1a_2a_3a_4a_5$, kjer je a_i bit, $a_i \in \{0,1\}$, i = 1,..,5.

Permutacijski ključ je tudi 5-bitni ključ:
$k_2 = b_1b_2b_3b_4b_5$, kjer je b_i bit, $b_i \in \{0,1\}$, i = 1,..,5.

Operaterji so spreminjali ključa v presledku treh do devet dni s spreminjanjem povezovalnih kablov.

$a_i \leftarrow w_j$ za nek i, j (operatorjev izbor) ... a_i dobi bit od kolesa w_j
$b_k \leftarrow w_l$ za nek k, l (operatorjev izbor) ... b_k dobi bit od kolesa w_l

Primer: Operator določi

$a_1 \leftarrow w_5 \quad a_2 \leftarrow w_4 \quad a_3 \leftarrow w_6 \quad a_4 \leftarrow w_7 \quad a_5 \leftarrow w_2$
$b_1 \leftarrow w_1 \quad b_2 \leftarrow w_3 \quad b_3 \leftarrow w_{10} \quad b_4 \leftarrow w_8 \quad b_5 \leftarrow w_9$

Postopek šifriranja nekega čistopisa x

1. Izberemo čistopis x.

2. Iz mednarodne telegrafske abecede št.2 CCITT2 dobimo 5-bitno kodo $x = x_1x_2x_3x_4x_5$, kjer $x_i \in \{0, 1\}$.

3. 5-bitno kodo šifriramo s ključem $k_1 = a_1a_2a_3a_4a_5$, tako:
   $x_1 \oplus a_1 = y_1$
   $x_2 \oplus a_2 = y_2$
   $x_3 \oplus a_3 = y_3$
   $x_4 \oplus a_4 = y_4$
   $x_5 \oplus a_5 = y_5$, kjer je $\oplus$ seštevanje po modulu 2.

4. Dobimo šifrirano 5-bitno kodo $y = y_1y_2y_3y_4y_5$.

5. y permutiramo s ključem $k_2 = b_1b_2b_3b_4b_5$ tako,da podamo permutacijsko pravilo:

   če je b_i=0, potem ne permutira, za vse i,
   če je b_1=1, potem zamenjata bita y_1 in y_2,
   če je b_2=1, potem zamenjata bita y_2 in y_3,
   če je b_3=1, potem zamenjata bita y_3 in y_4,
   če je b_4=1, potem zamenjata bita y_4 in y_5,
   če je b_5=1, potem zamenjata bita y_5 in y_1.

6. Dobimo permutirano šifrirano 5-bitno kodo z.

3.2 Primer šifriranja in dešifriranja

3.2.1 Šifriranje čistopisa

Predpostavimo, da imamo začetni položaj vseh koles:

Začetni korak:

tip kolesa	1	2	3	4	5	6	7	8	9	10
položaj	12	32	12	25	18	47	52	15	06	44
bit	1	0	1	1	0	1	1	0	1	0

Naslednji korak:

tip kolesa	1	2	3	4	5	6	7	8	9	10
položaj	13	33	13	26	19	48	53	16	07	45
bit	0	1	1	0	1	1	1	1	0	1

Naj bo $a = a_1a_2a_3a_4a_5$ aditivni ključ in $b = b_1b_2b_3b_4b_5$ permutacijski ključ.

Kolesi w_i naj bodo povezani:

kolo 1 $w_1 \to a_2$	kolo 2 $w_2 \to a_5$	kolo 3 $w_3 \to b_2$	kolo 4 $w_4 \to a_3$
kolo 5 $w_5 \to a_1$	kolo 6 $w_6 \to b_5$	kolo 7 $w_7 \to a_4$	kolo 8 $w_8 \to b_1$
kolo 9 $w_9 \to b_4$	kolo 10 $w_{10} \to b_3$		

Zdaj pa šifriramo "TO". Najprej šifriramo čistopis "T", ki je predstavljen s telegrafsko kodo 00001 iz mednarodne telegrafske abecede št.2.

Postopek šifriranja znaka "T"

1. x=00001.

2. Kolesa so v začetnem položaju. Prvi bit aditivnega ključa a_1 dobi vrednost s kolesa tipa 5 položaja 18; drugi bit a_2 dobi vrednost s kolesa tipa 1 položaja 12; tretji bit a_3 dobi vrednost s kolesa tipa 4 položaja 25; četrti bit a_4 dobi vrednost s kolesa tipa 7 položaja 52; peti bit a_5 dobi vrednost s kolesa tipa 2 položaja 32:

$$w_{1,12} = 1 \to a_2, a_2 = 1 \quad w_{2,32} = 0 \to a_5, a_5 = 0 \quad w_{4,25} = 1 \to a_3, a_3 = 1$$
$$w_{5,18} = 0 \to a_1, a_1 = 0 \quad w_{7,52} = 1 \to a_4, a_4 = 1.$$

Dobimo aditivnii ključ $a = a_1a_2a_3a_4a_5 = 01110$.

Prvi bit permutacijskega ključa b_1 dobi vrednost s kolesa tipa 8 položaja 15; drugi bit b_2 dobi vrednost s kolesa tipa 3 položaja 12; tretji bit b_3 dobi vrednost s kolesa tipa 10 položaja 44; četrti bit b_4 dobi vrednost s kolesa tipa 9 položaja 06; peti bit b_5 dobi vrednost s kolesa tipa 6 položaja 47:

$$w_{3,12} = 1 \to b_2, b_2 = 1 \quad w_{6,47} = 1 \to b_5, b_5 = 1 \quad w_{8,15} = 0 \to b_1, b_1 = 0$$
$$w_{9,06} = 1 \to b_4, b_4 = 1 \quad w_{10,44} = 0 \to b_3, b_3 = 0.$$

Dobimo permutacijski ključ $b = b_1b_2b_3b_4b_5 = 01011$.

3. x šifriramo s ključem a:

$$y_1 = x_1 \oplus a_1 = 0 \oplus 0 = 0,$$
$$y_2 = x_2 \oplus a_2 = 0 \oplus 1 = 1,$$
$$y_3 = x_3 \oplus a_3 = 0 \oplus 1 = 1,$$
$$y_4 = x_4 \oplus a_4 = 0 \oplus 1 = 1,$$
$$y_5 = x_5 \oplus a_5 = 1 \oplus 0 = 1.$$

Dobimo šifrirano 5-bitno kodo $y = y_1y_2y_3y_4y_5 = 01111$.

4. $y = 01111$ permutiramo s ključem $b = 01011$:

Najprej beremo prvi bit $b_1 = 0$, ker ima vrednost 0, se nič ne zgodi oz. ne permutira.

Potem beremo drugi bit $b_2 = 1$, ker ima vrednost 1, zamenja y_2 in y_3.
Tako dobimo $y_2 = 1$ in $y_3 = 1$.

Potem beremo tretji bit $b_3 = 0$, ker ima vrednost 0, se nič ne zgodi oz. ne permutira.

Potem beremo četrti bit $b_4 = 1$, ker ima vrednost 1, zamenja y_4 in y_5.
Tako dobimo $y_4 = 1$ in $y_5 = 1$.

Potem beremo peti bit $b_5 = 1$, ker ima vrednost 1, zamenja y_5 in y_1.
Tako dobimo $y_5 = 0$ in $y_1 = 1$.

Dobimo permutirano šifrirano kodo $z = 11110$.

S tem je šifriran "T" 00001 v 11110.
Telegrafska koda 11110 je predstavljena kot znak "K".

Za šifriranje naslednjega znaka se vsa kolesa premaknejo za eno mesto (npr. kolo tipa 1 položaja j se premakne za eno mesto v položaju j+1). Pri tem seveda dobimo povsem nov aditivni ključ in nov permutacijski ključ, ki imata lahko drugačne vrednosti kot prejšnji ključ (vrednost kolesa $w_{1,j}$ ni nujno enak $w_{1,j+1}$).

Postopek šifriranja znaka "O"

1. x=00011.

2. Kolesa so v začetnem položaju. Prvi bit aditivnega ključa a_1 dobi vrednost s kolesa tipa 5 položaja 19; drugi bit a_2 dobi vrednost s kolesa tipa 1 položaja 13; tretji bit a_3 dobi vrednost s kolesa tipa 4 položaja 26; četrti bit a_4 dobi vrednost s kolesa tipa 7 položaja 53; peti bit a_5 dobi vrednost s kolesa tipa 2 položaja 33:

$$w_{1,13} = 0 \to a_2, a_2 = 0 \quad w_{2,33} = 1 \to a_5, a_5 = 1 \quad w_{4,26} = 0 \to a_3, a_3 = 0$$
$$w_{5,19} = 1 \to a_1, a_1 = 1 \quad w_{7,53} = 1 \to a_4, a_4 = 1.$$

Dobimo aditivni ključ $a = a_1a_2a_3a_4a_5 = 10011$.

Prvi bit permutacijskega ključa b_1 dobi vrednost s kolesa tipa 8 položaja 16; drugi bit b_2 dobi vrednost s kolesa tipa 3 položaja 13; tretji bit b_3 dobi vrednost s kolesa tipa 10 položaja 45; četrti bit b_4 dobi vrednost s kolesa tipa 9 položaja 07; peti bit b_5 dobi vrednost s kolesa tipa 6 položaja 48:

$$w_{3,13} = 1 \to b_2, b_2 = 1 \quad w_{6,48} = 1 \to b_5, b_5 = 1 \quad w_{8,16} = 1 \to b_1, b_1 = 1$$
$$w_{9,07} = 0 \to b_4, b_4 = 0 \quad w_{10,45} = 1 \to b_3, b_3 = 1.$$

Dobimo permutacijski ključ $b = b_1b_2b_3b_4b_5 = 11101$.

3. x šifriramo s ključem a:

$$y_1 = x_1 \oplus a_1 = 0 \oplus 1 = 1,$$
$$y_2 = x_2 \oplus a_2 = 0 \oplus 0 = 0,$$
$$y_3 = x_3 \oplus a_3 = 0 \oplus 0 = 0,$$
$$y_4 = x_4 \oplus a_4 = 1 \oplus 1 = 0,$$
$$y_5 = x_5 \oplus a_5 = 1 \oplus 1 = 0.$$

Dobimo šifrirano 5-bitno kodo $y = y_1y_2y_3y_4y_5 = 10000$.

4. $y = 10000$ permutiramo s ključem $b = 11101$:

Najprej beremo prvi bit $b_1 = 1$, ker ima vrednost 1, zamenja y_1 in y_2.
Tako dobimo $y_1 = 0$ in $y_2 = 1$.

Potem beremo drugi bit $b_2 = 1$, ker ima vrednost 1, zamenja y_2 in y_3.
Tako dobimo $y_2 = 0$ in $y_3 = 1$.

Potem beremo tretji bit $b_3 = 1$,ker ima vrednost 1, zamenja y_3 in y_4.
Tako dobimo $y_3 = 0$ in $y_4 = 1$.

Potem beremo četrti bit $b_4 = 0$, ker ima vrednost 0, se nič ne zgodi oz. ne permutira.

Potem beremo peti bit $b_5 = 1$, ker ima vrednost 1, zamenja y_5 in y_1.
Tako dobimo $y_5 = 0$ in $y_1 = 0$.

Dobimo permutirano šifrirano kodo $z = 00010$.

S tem je šifriran "O" 00011 v 00010.
Telegrafska koda 00010 je predstavljena kot posebni znak CR(Carriage return - na začetek vrstice).

3.2.2 Dešifriranje tajnopisa

PRIMER

Dešifriranje tajnopisa znaka "K".

Tajnopis znaka "Z" je z=11110.

Znana sta aditivni ključ a=01110 in permutacijski ključ b=01011.

1. z=11110 permutiramo s ključem b=01011:

Najprej beremo peti bit $b_5 = 1$, ker ima vrednost 1, zamenja z_5 in z_1.
Tako dobimo $z_5 = 1$ in $z_1 = 0$.

Potem beremo četrti bit $b_4 = 1$, ker ima vrednost 1, zamenja z_4 in z_5.
Tako dobimo $z_5 = 1$ in $z_4 = 1$.

Potem beremo tretji bit $b_3 = 0$, ker ima vrednost 0, se nič ne zgodi oz. ne permutira.

Potem beremo drugi bit $b_2 = 1$, ker ima vrednost 1, zamenja z_2 in z_3.
Tako dobimo $z_2 = 1$ in $z_3 = 1$.

Potem beremo prvi bit $b_1 = 0$, ker ima vrednost 0, se nič ne zgodi oz. ne permutira.
Imamo permutiran y= 01111.

2. y=01111 šifriramo s šifrirnim ključem a=01110 po odštevanju po modulu 2:

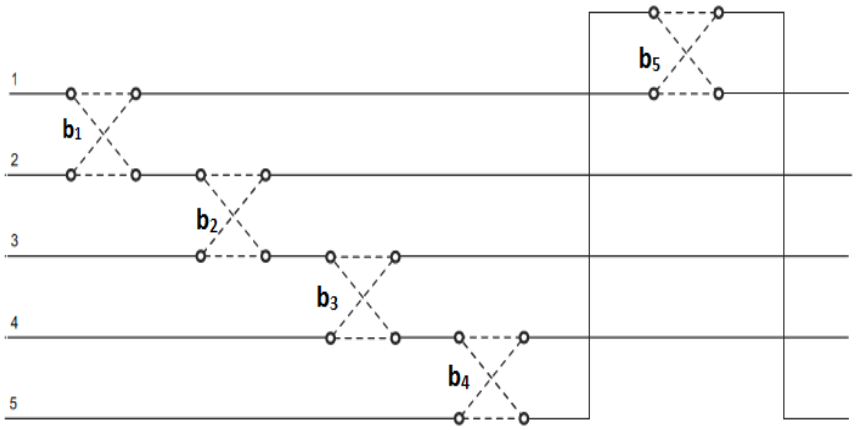
$$x = a \ominus y$$

$$\begin{aligned} x_1 &= a_1 \ominus y_1 = 0 \ominus 0 = 0 \\ x_2 &= a_2 \ominus y_2 = 1 \ominus 1 = 0 \\ x_3 &= a_3 \ominus y_3 = 1 \ominus 1 = 0 \\ x_4 &= a_4 \ominus y_4 = 1 \ominus 1 = 0 \\ x_5 &= a_5 \ominus y_5 = 1 \ominus 0 = 1 \end{aligned}$$

Dobimo x=00001, ki je predstavljen kot čistopis "T".

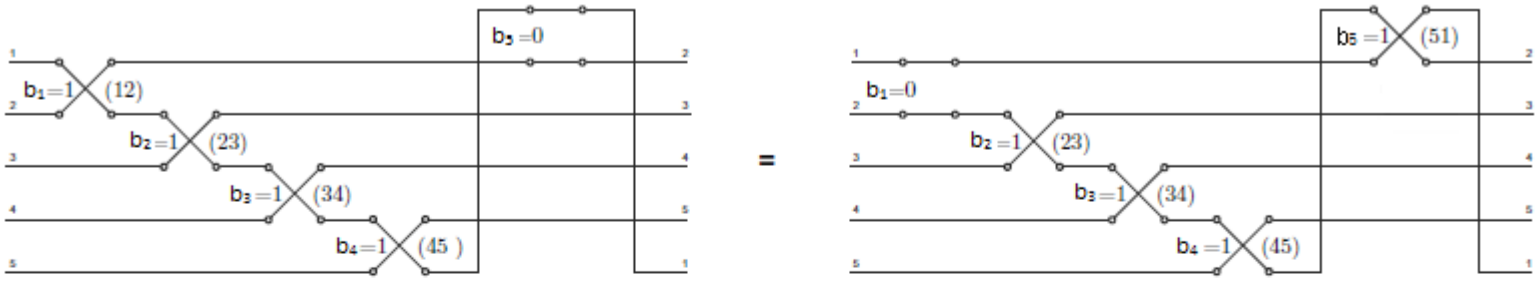
3.3 Permutacija

Permutacija s permutacijskim ključem $b_1 b_2 b_3 b_4 b_5$ v G-Schreiberju izgleda tako:

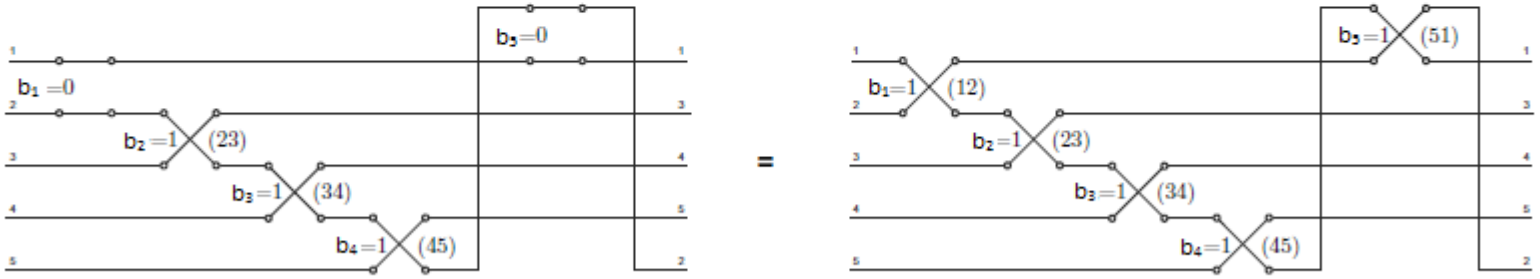


Poglejmo, koliko vseh možnih permutacij izvede G-Schreiber. Pričakovali bi, da je to $2*2*2*2*2 = 32$ vseh možnih permutacij. Dejansko obstaja le 30 možnih permutacij.

Spodnji diagram prikazuje potek permutacije linij, ki so na levi strani in so oštevilčene od 1 do 5. Te nakazujejo bite čistopisnih črk. Rezultat permutacije so biti tajnopisnih črk. Kot je to vidno na sliki 1 in sliki 2 križanje linij producira zamenjavo.



Slika 1: Identiteta $(12)(23)(34)(45) = (23)(34)(45)(51)$



Slika 2: Identiteta $(23)(34)(45) = (12)(23)(34)(45)(51)$

Zaradi tega je znotraj 32 izvedenih permutacij dejansko število različnih permutacij le 30. To lahko prikažemo na sledeči način: Zamenjava linij i in k je označena z (ik).

Zaradi

$(12)(23)(34)(45) = (23)(34)(45)(51) = (54321)$ (Glej sliko 1) in
$(23)(34)(45) = (12)(23)(34)(45)(51) = (5432)$ (Glej sliko 2),

število različnih permutacij ne more biti več kot 30. Dejansko lahko hitro ugotovimo, da je njihovo število 30.

3.4 Operater

V tem delu prispevka bomo opisali, kako poteka komunikacija med operaterjema pri pošiljanju skrivnega telegrama z uporabo G-Schreiberjevega stroja.

Pri pošiljanju sta aktivna dva operaterja, ki se nahajata na različnih lokacijah. Oba operaterja imata vsak svoj G-Schreiberjev stroj. Pri tem stroja morata imeti enako arhitekturo. Primer: G in H sta G-Schreiberja stroja; $g_{i,j}$ je vrednost kolesa tipa i položaja j stroja G, $h_{i,j}$ pa je vrednost kolesa tipa i poloaja j stroja H. G in H sta identična, če $g_{i,j} = h_{i,j}$ za vse i, j. Če pa G in H imata različne vrednosti npr. $\exists\ i, j : g_{i,j} \neq h_{i,j}$, potem bo eden izmed operaterjev dobil nepravilen telegram ter bi s tem povzročil nepravilno komunikacijo med tema operaterjema.

Za uspešno komunikacijo med dvema operaterjema morata operaterja imeti:

- Identična G-Schrebierja stroja (vse vrednosti vsakega kolesa za vse položaje so enaki)
- Pred začetkom šifriranja telegrama je potrebno, da imata operaterja isti indikatorski položaj vseh desetih koles. V primeru, če imata različen indikatorski položaj vsaj enega kolesa, potem operater, ki sprejema sporoilo ne more pravilno dešifrirati telegrama.
- Prav tako morata operaterja imeti enak povezovalni kabel med kolesom in relejem.

Poglejmo kako se operaterja dogovorita za določitev indikatorskiega položaja vseh desetih koles.

QEP in QEK sta števili, ki sta namenjeni za nastavitev položaja koles. Glede na to, da G-Schreiber ima 10 koles, obstaja 5 QEP in 5 QEK števil. QEK števila se ne spreminjajo tekom dneva. Pred začetkom pošiljanja sporočila imajo za vse poslane šifrirane telegrami znotraj 24-urnega obdobja enaka vsa QEK števila, namenjena za določitev indikatorskih položajev posameznih koles. QEP števila pa se spreminjajo za vsak poslan telegram. Operater, ki pošilja sporočilo sam izbira QEP števila.

Oba operaterja dnevno dobivata tabelo ključev, ki vsebujejo 5 QEK števila in 5 zaporednih pik. Pike so prostor za samostojno izbiro QEP števil s strani operatreja. V nadaljevanju je primer tabele ključev:

```
Kolo   1  2  3  4  5  6  7  8  9 10
Datum:
2.maj 12 32  .  .  .  .  . 15 06 44
3.maj 42 11 58 02  .  .  .  .  . 68
4.maj 22  .  .  .  .  . 67 30 58 62
5.maj 37 15 27 26 29  .  .  .  .  .
```

PRIMER

Oba operaterja imata dnevni seznam ključev kot je to razvidno iz zgornjega primera. V kolikor operater pošilja drugemu operaterju telegram dne 3.maja, potem samostojno izbere vrednost QEP tevila 12 25 18 47 52. Te vrednosti mora sporočiti drugemu operaterju. Pri naslednjem sporočilu dobi QEP števila drugega operaterja, ki mu pošilja novo sporočilo in te vrednosti QEP števil uporablja pri pošiljanju novega telegrama. Operaterja tako lahko pravilno nenehno komunicirata.

Pri izboru QEP števila 12 25 18 47 52 dne 3.maja je določen indikatorski položaj 42 11 58 02 12 25 18 47 52 68. Oba operaterja nastavita kolesa na ta položaj ter tako lahko pravilno komunicirata. Isti indikatorski položaj pri obeh G-Schreiberjih zagotavljata pravilno šifriranje vsakega telegrama.

◇

Vseh deset koles G-Schreiberja imajo periodo 47 53 59 61 64 65 69 71 in 73. Za vsak šifriran znak se vsa kolesa premaknejo za en korak. Zakaj je perioda imela taka števila?

Vidimo, da so vse kolesne periode med seboj tuja števila, kar pomeni, da nimajo skupnega faktorja. Celotna perioda G-Schreiber-ja tj. število korakov mora biti takšno, da omogoča vrnitev vseh koles na začetni položaj, je enaka produktu vseh posameznih kolesnih period $47*53*59*61*64*65*69*71*73 =$ 893 622 318 929 520 960 korakov.

Če bi te periode imele skupne faktorje, bi bila skupna perioda stroja manjša.

4 Razbitje G-Schreiberja

V tem poglavju je opisana Beurlingova analiza, s katero mu je uspelo razbiti kompleksno šifro v relativno kratkem času. Po kratkem uvodu je s pomočjo konkretnih primerov rekonstruiran možen potek razbitja šifre.

4.1 Uvod

Beurlingovo delo na področju dekodiranja G-Schreiberja je izredno učinkovito. Neverjetno je dejstvo, da mu je uspelo G-Schreiberjev algoritem dekodirati v komaj dveh tednih, saj je to bil kompleksen algoritem. Poleg tega Beurling na samem začetku ni imel nobenih izkušenj s funkcioniranjem teleprinterjev, sploh pa ne s principi teleprinterskega kodiranja. Najverjetneje se je seznanil s teleprinterji preko dostopne strokovne literature. Očitno je koristil svojo bistroumnosti in izvajal natančne analize razpoložljivih podatkov, kar ga je pripeljalo do učinkovitega odkritja vzorcev teleprinterskega kodiranja. Znano je, da so Beurlingove analize temeljile bolj na zdravem razumu oziroma razmišljanju kot na kompliciranih matematičnih enačbah. Pri svojem delu si je pomagal z izkušnjami operaterjev pri njihovem delu s sporočili. Neverjetno je, da so Beurlingovi največji zavezniki bili prav nemški operaterji, saj so se ti ubadali z velikim številom sporočil, z dolgimi telekomunikacijskimi linijami, s pogostimi prekinitvami in so pri svojem delu pogosto uporabljali nepreizkušene protokole. Najbolj pomembno je bilo dejstvo, da se niso zavedali posledic svojih poenostavitev in sprememb uveljavljenih rutin ter pravil. Po drugi strani pa se je Beurling dobro zavedal pomembnosti človeškega faktorja in njegove (ne)zanesljivosti. Vedel je, da je ravno to največkrat razlog "velike verjetnosti, da se možne napake tudi zgodijo".

4.2 Tehnika pošiljanja sporočil

Ni povsem jasno kako je potekalo natančno Beurlingovo dekodiranje sporočila dne 25.maja in 27.maja. Spodaj naveden zapis pa bi lahko bil verjeten potek glede na današnja spoznanja. Sporočilo s katerim se je srečal Beurling (sprejemno sporočilo) bi lahko imel takšen zapis:

HIER35MBZ35QRV54B35**KK35**QEP**4**5QW55WT55QI55RU55TW
3355553535UMUM35**VEVE35**ZRDDLH5FNY13QUKD4GEHNSWO...

4.2.1 Priprava izmenjave sporočil

Prvi korak je določanje pomena številk 3,4 in 5. Na osnovi spoznanj 2.poglavja (sl.1) v zgornjem zapisu 3,4 in 5 pomenijo LS-Letter Shift, FS-Figure Shift in SP-Space. Zapis in znaki v krepki pisavi pa prihajajo iz sprejemnika. S stališča kriptografije so znaki sprejemnika sestavni del kodiranega teksta. Zaradi pravilne analize se ti morajo vključiti v tekst pošiljatelja čeprav so bili poslani preko različnega kanala.

Na oddajni strani so izmenjave imele nekoliko drugačen zapis:

HIER MBZ QRV? **KK** QEP 12 25 18 47 52 UMUM **VEVE** ...

Začetek izmenjave je v čistopisu in je razvidna identifikacija pošiljatelja – "MBZ" je identifikacija postaje. Znak "QRV" iz zgornjega teksta je vprašanje razumevanja izmenjave. Na drugi strani sledi odgovor, ki je zapisan kot "KK"(kar pomeni *klar* oz. "jasno").

Nato sledi prenos QEP števil.

Potem se izmenjava prekine ker operaterji na obeh straneh nastavljajo QEP števila.

4.2.2 Izmenjava

Kodirana izmenjava začne na oddajni strani z napisom **"UMUM"** (pomeni **umschalten** oziroma preklop). V nadaljevanju sprejemnik odgovori **"VEVE"**, kar je znak za **verstanden** oziroma razumem. Po tej izmenjavi se naprava na obeh straneh preklopi na "kripto". Operaterji bi morali pred potekom resničnega oddajanja sporočila še enkrat preveriti varnost tako, da ponovijo nekatere oznake iz čistopisa kot je npr. "QRV" ali podobno. In ravno v tem delu postopka je največkrat prihajalo do nepravilnosti in nedoslednosti.

4.3 Beurlingova kriptoanaliza

Zaporedje čistopisa "35" je predstavljena kot presledek med besedami. Presledek je v vsakem besedilu telegrama razumljivo najbolj pogosto uporabljen.
Zakaj "35", ne "5" kot ima pomen v mednarodni telegrafski abecedi št.2 CCITT2?
Telegrafske linije so bile dolge, včasih slabe, in zato pogosto izpostavljene interferenci, ki lahko izkrivlja posredovan znak. Prepoznavnost kljub temu ni bila motena, razen če se je znak spremenil v "4" (=figure shift), ker so potem vsi naslednji teksti postali nerazumljivi zaradi sprememb črk v številke in ločila. Če se je izkrivljanje dogajalo samo na sprejemni postaji, oddajna postaja ni opazila ničesar in je nadaljevala s popačenim prenosom. Da bi zmanjšali težave, operaterji so običajno uporabili za presledek "35" (=letter shift, space) namesto "5". Če bi ponovno prišlo do napake "4", bi se pomen presledka ponovno vzpostavil na pravilnem mestu.

Zdaj pa poglejmo, kako je Arne Beurling uspelo razbiti G-Schreiber.

PRIMER:

Spodaj je primer 10 telegramov, v katerih so bila šifrirana sporočila z istim ključem

1 ALZGJ1GUH4HJPLHN6N5BVE3CQUHGFBJN...
2 NP3UMWFZ31NMYKMJHB625FMQUHFDFZ45...
3 GRQUMAA4JTQFLQMHJIEGTVFWPOI32SLK...
4 LYZGJ1ORYYDRQKNHJN51AKFD5VCERWRV...
5 LEZGKVRVANBWE6MJUTGBTRV36H4H1CS1...
6 BOTA3WFUSGODA2JIUNYKRIYYTSFSCOGB...
7 YEYZL42DYD5LMHLOIMUQTGE5SHBZSHEB...
8 RKZGBWFLIX6AZEMKEY4DWOMBOCXQ6LBL...
9 CCNRWWGKOTV5LLUMCD3E4R3IYHJASLA6...
10 1TXUMSMU4VVNTZJNFIW35SDEDOTPMAND...

Stolpec	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Telegram														
1	A	L	Z	G	J	M	G	U	H	4	H	J	P	L
2	N	P	3	U	M	W	F	Z	3	1	N	M	Y	K
3	G	R	Q	U	M	A	A	4	J	T	Q	F	L	Q
4	L	Y	Z	G	J	M	O	R	Y	Y	D	R	Q	K
5	L	E	Z	G	K	V	R	V	A	N	B	W	E	6
6	B	O	T	A	3	W	F	Z	3	1	O	D	A	2
7	Y	E	Y	Z	L	4	2	D	Y	D	5	L	M	H
8	R	K	Z	G	B	W	F	L	I	X	6	A	Z	E
9	C	C	N	R	W	W	G	K	O	T	V	5	L	L
10	1	T	X	U	M	S	M	U	4	V	V	N	T	Z

Beurling je hitro odkril, da se znaki ponavljajo v nekem stolpcu telegramov. To kaže na dejstvu, da so bili telegrami šifrirani z istim ključem in na dejstvo, da je večina telegramov začenjala z enako - pogosto formalistično - besedo. Večkrat ponavljajoči znaki po začetnih stolpcih, takoj izza formalističnih besed, kažejo na presledek "35". Da bi lahko potrdil te domneve, je poskušal razlikovati med tajnopisi iz istega stolpca, da bi lahko preveril, če sta tajnopisa v resnici presledek.

Primer: Analiza pri četrtem stolpcu.

Vidimo, da imata "3" in "5" en skupen bit na tretjem položaju:

3=11111
5=00100.

Kako potrditi pravilnost domneve?

Ker imajo telegrami isti ključ, poglejmo, kakšna je razlika tajnopisa "3" in "5".

Naj bo k_1 aditivni ključ in k_2 permutacijski ključ

$$11111 \oplus k_1 = y_1$$
$$00100 \oplus k_1 = y_2.$$

y_1 in y_2 imata spet en skupen bit za poljubni k_1.

y_1 in y_2 permutiramo za poljubni k_2 ter tako permutirana y_1 in y_2 imata tudi en skupen bit.

Od tod sledi, da tudi tajnopis od "3" in tajnopis od "5" imata en skupen bit. Če pa tajnopisa nimata enega skupnega bita, potem ovržemo domnevo, da imata pomen presledka.

Zdaj pa poglejmo, kako je Beurling dešifriral tajnopisa "G" in "U" v četrtem stolpcu kot rezultat "3" in "5".

Primerjava: (čistopis) "3": 11111 (tajnopis) "G": 01011
(čistopis) "5": 00100 (tajnopis) "U": 11100,

pokaže, da "G" in "U" imata skupen bit samo na drugem položaju ter "3" in "5" imata skupen bit samo na tretjem položaju.
To nakazuje, da je permutacija definirana tako, da premakne bit iz tretjega položaja na drugi položaj.

Da je y tajnopis v resnici bil šifriran od x čistopisa, mora veljati enačba:

$$\pi^{-1}(y) = x \oplus k,$$

kjer je y tajnopis, x čistopis.

Potem je x pravi čistopis. Če ne velja, potem x ni pravi čistopis.

Permutacija naj bo

$\pi = (23)$. $3 : x = 11111$ $G : y = 01011$
$11111 \oplus k = 00111$
$k = 11000$.

Beurling je našel pravi ključ, ki zadošča pogoju. Ko je Beurling našel ključ za četrti stolpec, je lahko brez težav dešifriral še preostale tajnopise, ki so v četrtem stolpcu.

Na podoben način kot za četrti stolpec je Beurling odkril, da so tudi v petem in šestem stolpcu presledki.

Stolpec 5: "J" 11010 Stolpec 6: "W" 11001
"M" 00111 "1" 00010
"J-M" ter "W-1" imata en skupen bit.

Tako je Beurling odkril ključ za četrti, peti in šesti stolpec. Dešifriral je "G","U" v četrtem stolpcu, "J","M" v petem stolpcu in "M","1" v šestem stolpcu. Prav tako je dešifriral tajnopise v tretjem stolpcu, ko je v četrtem stolpcu že odkril "5" pri istem telegramu. Nato je dešifriral tudi tajnopise v sedmem stolpcu, ko je v šestem stolpcu že odkril "3".

Spodaj je zgled trenutno delno dešifriranega telegrama:

Stolpec	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Telegram														
1	A	L	Z	G	J	M	G	U	H	4	H	J	P	L
			3	5	3	5								
2	N	P	3	U	M	W	F	Z	3	1	N	M	Y	K
				3	5	3	5							
3	G	R	Q	U	M	A	A	4	J	T	Q	F	L	Q
				3	5									
4	L	Y	Z	G	J	M	O	R	Y	Y	D	R	Q	K
			3	5										
5	L	E	Z	G	K	V	R	V	A	N	B	W	E	6
			3	5										
6	B	O	T	A	3	W	F	Z	3	1	O	D	A	2
						3	5							
7	Y	E	Y	Z	L	4	2	D	Y	D	5	L	M	H
8	R	K	Z	G	B	W	F	L	I	X	6	A	Z	E
			3	5		3	5							
9	C	C	N	R	W	W	G	K	O	T	V	5	L	L
10	1	T	X	U	M	S	M	U	4	V	V	N	T	Z
				3	5									

Zdaj pa poglejmo, kako se je Beurling lotil sedmega stolpca.

Na začetku vsakega telegrama se "Q","R" in "V" pogosto pojavljajo. Zato je koristno poznavanje razlike med "3-V", "3-Q" in "Q-R".

Vidimo, da "3-V":

11111 (3)
01111 (V) imata 4 skupne bite, 1 različen bit,

"3-Q":

11111 (3)
11101 (Q) imata 4 skupne bite, 1 različen bit,

"Q-R":

11101 (Q)
01010 (R) imata 1 skupen bit, 4 različne bite.

Najprej je treba uganiti, kje se je začel QRV. Vidimo, da v telegramu št. 5, digrafu "35" ne sledi "35". Na osnovi primerjave z telegramom št. 4 v petem stolpcu

"J" 11010
"K" 11110

ima 4 skupne bite in 1 različen bit, kar namiguje na to, da je lahko "K" v resnici "Q". Razlika "3-Q" ima 4 skupne bite in 1 različen bit, zato tudi razlika "J-K" mora biti enaka.

Na spodnji razpredelnici so prikazani delno dešifrirani telegrami, ki jih je Beurling dopolnil še z QRV.

Stolpec	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Telegram														
1	A	L	Z	G	J	M	G	U	H	4	H	J	P	L
			3	5	3	5	3	5	3	5				
2	N	P	3	U	M	W	F	Z	3	1	N	M	Y	K
				3	5	3	5	Q	R	V				
3	G	R	Q	U	M	A	A	4	J	T	Q	F	L	Q
				3	5	Q	R	V						
4	L	Y	Z	G	J	M	O	R	Y	Y	D	R	Q	K
			3	5	3	5	Q	R	V					
5	L	E	Z	G	K	V	R	V	A	N	B	W	E	6
			3	5	Q	R	V	3	5					
6	B	O	T	A	3	W	F	Z	3	1	O	D	A	2
						3	5							
7	Y	E	Y	Z	L	4	2	D	Y	D	5	L	M	H
8	R	K	Z	G	B	W	F	L	I	X	6	A	Z	E

			3	5		3	5							
9		C	C	N	R	W	W	G	K	O	T	V	5	L	L
10		1	T	X	U	M	S	M	U	4	V	V	N	T	Z
					3	5								

Za pravilnost Beurlingove hipoteze se moramo prepričati s pomočjo primerjav razlik "3-5", "3-Q", "Q-R" in "3-V" tako, da dobimo pravilen ključ. Če ne moremo dobiti ključa, je hipoteza ovržena ter je potrebno ugibati na drugačen način.
Vidimo, da se v sedmem stolpcu pojavljajo "3","5","Q","R","V" ter zato naredimo primerjavo "3-5", "3-Q", "Q-R" in "3-V" v sedmem stolpcu.

"3-5":
(čistopis) "3": 11111 (tajnopis) "G": 01011 "3-5" in "G-F" imata en skupen bit
(čistopis) "5": 00100 (tajnopis) "F": 10110

Ker imata "3-5" skupen bit v tretjem položaju in "G-F" pa v četrtem položaju, je permutacija 3→4.

"3-Q":
(čistopis) "3": 11111 (tajnopis) "G": 01011 "3-Q" in "G-O" imata en različen bit
(čistopis) "Q": 11101 (tajnopis) "O": 00011

Ker imata "3-Q" različen bit v četrtem položaju in "G-F" pa v drugem položaju, je permutacija 4→2 .

"3-V":
(čistopis) "3": 11111 (tajnopis) "G": 01011 "3-V" in "G-R" imata en različen bit
(čistopis) "V": 01111 (tajnopis) "R": 01010

Ker imata "3-V" različen bit v prvem položaju in "G-R" pa v petem položaju, je permutacija 1→5 .

"R-Q":
(čistopis) "R": 01010 (tajnopis) "A": 11000 "R-Q" in "A-O" imata en skupen bit
(čistopis) "Q": 11101 (tajnopis) "O": 00011

Ker imata "R-Q" skupen bit v drugem položaju in "A-O" pa v tretjem položaju, je permutacija 2→3 .

Še dodamo eno permutacijo 5→1. Dobimo končno permutacijo:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 2 & 1 \end{pmatrix} = (15)(234).$$

Izračunajmo aditivni ključ za sedmi stolpec.

$\pi = (15)(234)$.

Naj bo x čistopis, y tajnopis, k aditivni ključ

$x = 3$, $y = G$
$y = \pi(x \oplus k)$
$G = \pi(3 \oplus k)$
$01011 = \pi(11111 \oplus k)$
$\pi^{-1}(01011) = 11111 \oplus k$
$111000 = 11111 \oplus k$
$k = 00011$.

Aditivni ključ je 00011.

Zdaj poglejmo, ali velja aditivni ključ k za "Q","R","V".

"Q" :
$x = Q$
$y = 0$
$k = 00011$
$0 = \pi(Q \oplus k)$
$00011 = \pi(10100)$
$00011 = 00011$ Pravilen!

"R":
$x = R, y = A, k = 00011$
$A = \pi(R \oplus k)$
$11000 = \pi(01010 \oplus 00011)$
$11000 = \pi(01001)$
$11000 = 11000$ Pravilen!

"V" :
$x = V, y = R, k = 00011$
$R = \pi(V \oplus k)$
$01010 = \pi(01100)$
$01010 = 01010$ Pravilen!

S tem smo pokazali, da je bila Beurlingova domneva pravilna. Tako smo dobili permutacijo in aditivni ključ za sedmi stolpec. Ker imamo ključ za sedmi stolpec, lahko dešifriramo vse tajnopise v vsakem telegramu pri sedmem stolpcu.
Beurlingov cilj je pridobiti vse ključe in permutacijo za vsak stolpec ter s tem lahko s pomočjo ključa dešifrirat celoten šifriran telegram.

Konec primera.

Znaki, ki so najbolj pogosto zasedali prva mesta v teleprinterski kodi so: "3", "5", "Q", "R", "V". Beurling je za njihovo prepoznavanje notiral sistem označb – pike za 1 in kroge za 0, in je diferenca binarnih zapisov posameznih znakov:

"3-5" **..o..**
"3-Q" **ooo.o**
"3-R" **.o.o.**
"3-V" **.oooo**
"5-Q" **..oo.**
"5-R" **o...o**
"5-V" **o.o..**
"$Q-R$" **.o...**
"$Q-V$"**.oo.o**
"$R-V$"**oo.o.**

Beurling je pri svojem delu predpostavljal, da znaki kot so **o....** , **.o...** , **..o..** , **...o.** , **....o** lahko pomenijo "3-5" oziroma "Q-R". Vedel je, da večkratni pojav enako spremenjenih znakov v istem stolpcu predstavlja večjo verjetnost, da je uporabljena enaka permutacija v vseh telegramih. Tako na primer v kolikor se je pojavil V, je verjel, da so "3" in "5" možni, "Q" in "R" pa je lahko eliminiral.

Čistopis razlike *"3-5":* **..o..** *"3-Q":* **ooo.o** *"Q-R":* **.o...** *"3-V":* **.oooo**
Tajnopis razlike *"G-F":* **...o.** *"G-O":* **o.ooo** *"O-A":* **..o..** *"G-R":* **oooo.**

Ta način, ki temelji na diferencah binarnih zapisov posameznih znakov je učinkovit za odkrivanja položajev za najbolj pogoste črke (znake) nemščine kot so npr. "E", "S", "A", "T","N".

Obilno število telegramov je bilo šifrirano z istim ključem. Velikokrat se je zgodilo, da so poslali od 20 do 40 telegramov z istim ključem, kar je v nasprotju z protokolom, ki bi moral za vsak telegram izbrati nov, spremenjen ključ. Operaterji so bili navadni vojaki, izšolani za hitro delo s teleprinterji, manj pa teoretično podkovani o posledicah morebitnega neupoštevanja navodil o izvajanju kriptografskih procesov. Zaradi obilice sporočil najpogosteje nepomembnih, so hitro zapadli v rutino in so samovoljno začeli opuščati posamične varnostne ukrepe. To je bila največja pomoč za kriptografe nasprotne strani. Tako je tudi Arne Beurlingu uspelo razbiti šifro G-Schreiber-ja. Na koncu s pomočjo veliko odkritih telegramov je Beurlingu uspelo rekonstruktirati G-Schreiberjev stroj in zgraditi popolno repliko G-Schreiberja.

Slika 4: Replika G-Schreiber

5 Zaključek

Beurlingova kriptoanaliza teleprinterskega kodirnega stroja G-Schreiberja je veliko prispevala k temu, da so Švedi dešifrirali veliko skrivnih sporočil, ki so jih Nemci pošiljali iz G-Schreiberja. Posledica teh odkritja sporočil je, da so Švedi vnaprej vedeli, kaj bodo Nemci počeli v bližnji prihodnosti. Razkrili so načrtovane vojaške operacije med drugimi tudi datum pričetka operacije "Barbarossa" (kodno ime za invazijo oboroženih sil Sil osi na Sovjetsko zvezo 22.junija 1941).

Razbitje šifre drugega nemškega stroja "Enigma" in japonskega stroja "Pubble" je bila zelo pomembna protiobveščevalna zmaga med drugo svetovno vojno. V primerjavi s tem je bilo razbitje G-Schreiberja, ki so ga dosegli na Švedskem, manj javno izpostavljeno ter kljub velikemu intelektualnemu trudu neznatno prispevalo vojaškim odločitvam. Toda iz švedske perspektive je bila pomembna v celotnem vojaško-političnem naporu za utrjevanje nevtralnosti in s tem izogibanje vojni na lastnem ozemlju.

Ocenjujemo, da je opisano dogajanje povezano z razbitjem G-Schreiberjeve kode imelo pomemben vpliv tudi na razvoj kriptografske znanosti. Ta ocena temelji na spoznanju, da je Beurling s svojim takratnim delom v praksi potrdil nekatere, danes pomembne, principe kriptografske znanosti. V nadaljevanju navajamo nekatera:

1. Potrjeno je zgodovinsko dejstvo, da je za uspešno vodenje socialnih družb oziroma držav pomembno skrivati vsebino določenih sporočil, kar še posebej velja za izredna stanja kot je stanje vojne, ko sporočila lahko imajo dramatičen vpliv na dogajanje v družbi oziroma državi, pa tudi širše.

2. Kriptografija nam lahko, ko jo pravilno implementiramo in uporabljamo, nudi največjo stopnjo varnosti pri zaščiti pomembnih sporočil, saj je to veda o komunikaciji, ki nas nenehno opozarja, da je pri komunikaciji vedno lahko prisoten aktiven napadalec. In vedno obstaja možnost, da bi napadalec bil tako genialen kot je to bil Beurling v našem primer. Za napad na G-Schreiber kriptosistem je imel le tajnopis, kar je najtežji način napada zaradi pomanjkanja informacij. Za Beurling je to bilo dovolj.

3. Pri razbijanju klasičnih šifer je potrebno upoštevati Kerckhoffov princip, ki pravi, da "nasprotnik lahko spozna kriptosistem oziroma algoritme, ki jih uporabljamo, ne pa tudi ključe, ki nam zagotavljajo varnost". Beurlingu je uspelo učinkovito razbitje G-Schreiber kode, saj je bil izreden matematik in dober poznavalec pomembnih gradnikov kriptografije. Zato je pomembno, da kriptografske sisteme kontroliramo s pomočjo ključev.

Literatura:

[1] Bengt Beckman: *Codebreakers:Arne Beurling and the Swedish crypto program during World War II*

[2] http://en.wikipedia.org/wiki/Arne_Beurling

[3] Lars Ulfving and Frode Weierud: *The Geheimschreiber Secret:Arne Beurling and the Success of Swedish Signals Intelligence*

[4] Friedrich Ludwig Bauer: *Decrypted Secrets: Methods and Maxims of Cryptology*

[5] http://en.wikipedia.org/wiki/Siemens_and_Halske_T52