

18 WERKBLAD PLAYFAIR

inleiding en sleutel maken

Het Playfair-cijfer is niet bedacht door Lyon Playfair, maar door Charles Wheatstone die het vernoemde naar zijn vriend. Het maakt gebruik van een sleutel in de vorm van een 5×5 raster, ofwel met 25 velden. Ons alfabet heeft 26 letters. Dit wordt opgelost door de *i* en de *j* gezamenlijk één veld te geven of door de *q* weg te laten. Op dit werkblad kiezen we voor het laatste.

Het raster wordt met behulp van een sleutelwoord als volgt opgebouwd:

b	a	r	n	w
o	d	c	e	f
g	h	i	j	k
l	m	p	s	t
u	v	x	y	z

FIGUUR 1

- I. Spreek een geheim sleutelwoord af.
In dit voorbeeld gebruiken we de geboorteplaats van Wheatstone: "barnwood".
- II. Vul het vierkant van boven naar beneden met de letters van het sleutelwoord. Zorg ervoor dat elke letter slechts één keer voorkomt.
- III. Vul het vierkant verder aan met de resterende letters van het alfabet (op volgorde van het alfabet).
Volgens afspraak slaan we de *q* over.

Dit leidt tot de sleutel in figuur 1.

berichten versleutelen

Stel dat Wheatstone het bericht "de stereoscoop is klaar" wil versleutelen, voor hij het naar Playfair stuurt.

1	d	e	s	t	e	r	e	o	s	c	o	o	p	i	s	k	l	a	a	r		
2	d	e	s	t	e	r	e	o	s	c	o	x	o	p	i	s	k	l	a	a	r	
3	d	e	s	t	e	r	e	o	s	c	o	x	o	p	i	s	k	l	a	x	a	r

FIGUUR 2

Het algoritme is als volgt:

- I. Deel de klare tekst op in digrammen: combinaties van twee letters. Als hierbij een digram met twee dezelfde letters ontstaat, voeg je een extra *x* toe tussen de twee gelijke letters.
in figuur 2 is dit proces in drie stappen te zien. Als de letters in paren van twee worden neergezet, zien we twee plaatsen met twee identieke letters. Alleen de *oo* is daarvan een digram. Volgens het algoritme voegen we daarom een *x* toe. In stap 2 is te zien dat hierdoor de *aa* die in eerste instantie geen digram was, nu wel een digram wordt. Daarom voegen we ook daar een *x* toe.
- II. Voor alle digrammen geldt nu één van de volgende drie mogelijkheden:
 - a. beide letters staan in dezelfde rij
 - b. beide letters staan in dezelfde kolom
 - c. geen van beide: a. en b. gelden beide niet.
- III. Deze drie mogelijkheden hebben hun eigen manier van afhandelen:
 - a. Vervang de letters door de letters direct rechts. Staat een letter aan het eind van de rij? Dan ga je terug naar het begin van de rij. *st* → *tl* (zie figuur 3)
 - b. Vervang de letters door de letters er direct onder. Staat een letter onderaan de kolom? Dan ga je terug naar het begin van de kolom.
 - c. Vervang de letters van het digram door de letter die je vindt op het kruispunt van de rij van deze letter en de kolom van de andere letter uit het digram.
er → *cn* (zie figuur 3)

b	a	r	n	w
o	d	c	e	f
g	h	i	j	k
l	m	p	s	t
u	v	x	y	z

FIGUUR 3

Opdracht A vercijferen met het Playfair-cijfer

1. Is het Playfair-cijfer een voorbeeld van transpositie- of substitutieversteuteling?
2. Hieronder zie je de boodschap van Wheatstone uit de theorie. Gebruik de sleutel uit figuur 1 / 3 om het bericht verder te versteutelen.

1	d	e	s	t	e	r	e	o	s	c	o	o	p	i	s	k	l	a	a	r		
2	d	e	s	t	e	r	e	o	s	c	o	x	o	p	i	s	k	l	a	a	r	
3	d	e	s	t	e	r	e	o	s	c	o	x	o	p	i	s	k	l	a	x	a	r
4	c	f	t	l	c	n																

Opdracht B het hele proces van versteutelen

Playfair stuurt een antwoord terug naar Wheatstone. Ze hebben afgesproken dat hiervoor standaard het sleutelwoord "calcutta" (een woonplaats van Playfair) te gebruiken.

3. Gebruik dit sleutelwoord om het raster hiernaast te vullen en hiermee de sleutel voor communicatie te genereren.

Playfair verstuurt een bericht door de klare tekst "die probeer ik graag hoor" te versteutelen.

4. Vul onderstaand schema in en bepaal op die manier de cijfertekst die Playfair naar Wheatstone stuurt.

klare tekst	d	i	e	p	r	o	b	e	e	r	i	k	g	r	a	a	g	h	o	o	r	
digrammen																						
cijfertekst																						

Opdracht C een versteuteld bericht ontcijferen

Playfair stuurt nog een bericht naar zijn vriend. Vanwege zijn Schotse afkomst kiest hij voor het sleutelwoord "whiskyproducent".

Playfair maakt weer een sleutel met behulp van het sleutelwoord. Als Playfair zijn klare tekst versteuteld met het gevonden 5 x 5 raster, leidt het algoritme tot de cijfertekst "WLUNUSUGURTYOGUSJGLGU".

5. Bedenk zelf hoe je in het algemeen een met Playfair vercijferd bericht kunt ontcijferen.
6. Gebruik het sleutelwoord om het raster hiernaast te vullen en hiermee de sleutel voor communicatie te genereren.
7. Ontcijfer de cijfertekst met behulp van de gevonden sleutel.

<i>klare tekst</i>																						
<i>digrammen</i>																						
<i>cijfertekst</i>	w	l	u	n	u	s	u	f	g	u	r	t	y	o	g	u	s	j	g	l	g	u