



Lønskrift eller Kryptografi

Af 46, 9, 4 - 57, 3, 5

III.

Willards System

Der existerer en Mængde Systemer, i hvilke Principet er det samme som i det, vi beskrev i den forrige Artikel. Den, der ønsker at gjøre Bekjendskab med flere saadanne, kunne vi henvise til Lindenfels: "Den hemmelige Skrivekunst" (Kbhvn 1819); vi ville her kun beskrive saadanne, der paa Grund af den Anvendelse, de have havt i Praxis, eller paa Grund af deres Særegenheder synes os at fortjene nærmere Omtale.

Det „Willardske” System er et Transpositionssystem, der slutter sig temmelig nær til le carré indéchiffable, men som ikke fordrer en saa stor Tabel. Dette

System blev anvendt af vore Diplomater til for kort Tid siden, da det blev afløst af Hr. Orloffs System, som vi senere komme til.

Vi hidsætte [...] den Tavle som anvendes ved Chiffreringen.

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

Man seer let, hvorledes denne Tavle er konstrueret. I den øverste Række staa Bogstaverne fra a til n (inkl.). I den forreste Række skrive vi fra a de følgende Bogstaver b, c o. s. v. nedefter, idet vi springe hvert andet Felt over; vi ende da forneden med o og skrive nu de følgende Bogstaver i Alfabetet op efter paa de ledige Pladser. Vi have herved det første Bogstav i hver Række, og nu udfylde vi

de horisontale Rækker, idet vi begynde med det allerede skrevne Bogstav og fortsætte i alfabetisk Orden, saaledes at vi, naar vi have naaet ø, begynde forfra. Dersom vi i vor Tavle i forrige Artikel havde brugt de 28 Bogstaver, som vi bruge her, kunde vi have dannet denne Tavle ved kun at bruge den første Halvdel af hver af de horisontale Rækker og herpaa flytte disse Rækker om i den nye Orden. Vi kunne lægge Mærke til, at den nederste Række indeholder de Bogstaver af Alfabetet, som den øverste mangler.

Man kunde nu godt bruge Tabellen, som den er, men man har fundet det bekvemmere at have hver vertikal Række for sig. Dersom vi klippe vor Tabel itu efter de vertikale Linier, faae vi 14 Strimler; klistrer man disse paa Pap eller Træ, har man et Apparat som det, der har været anvendt i vore Ministerier.

De udhævede Bogstaver øverst og nederst paa hver Strimmel bruges som Nøglebogstaver: Er Nøglen f. Ex. „Danmark”, lægger man de Strimler ved Siden af hinanden, hvis Mærkebogstaver danne dette Ord. Da Bogstaverne efter n staa nederst, bliver en saadan Seddel vendt om, naar den bruges, og Bogstaverne i den kommer til at staa paa Hovedet, hvis man ikke foretrækker at have Bogstaverne dobbelte som Herrebladene i et Spil Kort eller at fortsætte de horisontale Rækker helt ud, saa at man faaer 28 Strimler. Naar det samme Bogstav forekomme flere Gange i Nøglen, bruges det kun første Gang.

Vi have nu altsaa følgende Sedler liggende:

d	a	n	m	r	k
e	b	o	n	s	l
c	ø	m	l	q	j
f	c	p	o	t	m
b	æ	l	k	p	i
g	d	q	p	u	n
a	z	k	j	o	h
h	e	r	q	v	o
ø	y	j	i	n	g
.
.
.
.

hvor vi dog have skrevet Bogstaverne paa den næstsidste i deres naturlige Stilling i Stedet for vendte paa Hovedet.

Man bruger nu kun disse Sedler til Chifreringsen med denne Nøgle. Da hver Seddel har alle Alfabetets Bogstaver, kan det første Bogstav findes paa den første Seddel, det andet paa den anden o. s. v., og man skriver da i Depechen det Bogstav, der paa Sedlen staaer et bestemt (aftalt) Antal Pladser over eller under det givne Bogstav. Vi ville f. Ex. skrive

. . . der som før Kong . . .

og antage, at det er aftalt, at man skal bruge det Bogstav, der paa Sedlen staaer lige under det givne Bogstav. Under d paa den første Strimmel staaer e, under e paa den anden staaer y, under r paa den tredje j, under k paa den fjerde p, under o paa den femte v, under m paa den sidste i; nu er Nøglen opbrugt, og vi begynde forfra; vi have saaledes

. . . eyjpv – ibcjp – vha . . .

Dersom man ved at tælle nedefter eller opefter ikke finder Pladser nok, fortsætter man fra Sedlens anden Ende; saaledes staaer paa Sedlen a Bogstavet p 2 Pladser over a, Bogstavet d 6 Pladser under o og 8 Pladser under n. Havde altsaa Aftalen ovenfor været, at man skulde bruge Bogstavet tre Pladser over det, man har i Klarskriften, havde man faaet

. . . qæln – kdoln – tjc . . .

Den, der modtager Depechen og har Nøglen, lægger Sedlerne ud paa samme Maade og bærer sig nu ganske saaledes ad med Depechen, som Afsenderen gjorde med Klarskriften, blot at han tager Bogstavet lige saa mange Pladser over, som den anden tog det under, og omvendt; paa denne Maade maa han komme tilbage til de Bogstaver, som Afsenderen gik ud fra, og det er jo netop disse Bogstaver, han skal kjende. Den, der bruger Tabellen, som den er, maa naturligvis huske, at han ved Benyttelsen af de Rækker, hvor Nøglebogstavet staaer forneden, maa tælle lige saa mange Pladser nedefter, som han eller skal tælle opefter, og omvendt.

Spørgsmaalet er nu, om Hemmeligheden er sikkert skjult for den, der ikke kjender Nøglen, naar man anvender dette System. Vi skulle se, at dette er saa langt fra at være Tilfældet, at man her, ligesom ved det forrige System, kan være temmelig sikker paa at finde Løsningen, naar man blot har en Depeche, der er saa lang, at Nøglen er brugt 15 à 20 Gange. **Det er her som hist det Periodiske, der er Systemets svage Side.** Dersom man paa Sedlerne skal tælle mange Pladser over

eller under det givne Bogstav, vil det blive meget besværligt at bruge Systemet, og man vil risikere hyppige Fejltagelser. Vi ville derfor forudsætte, at man aldrig gaaer mere end højst 5 Pladser over eller under det givne Bogstav; derved undgaa vi nogen Vidtløftighed i det Følgende og faae dog viist Methoden saa fuldstændig, at Enhver selv let vil kunne udvide den til saadanne Tilfælde, hvor man ogsaa maa tage den Mulighed i Betragtning, at man kan have benyttet de større Afstande ved Chifreringsen.

Paa Grund af Tavlens Indretning kommer det væsenlig an paa, om man er gaaet et lige eller et ulige Antal Pladser over eller under det givne Bogstav.

I. Antallet af Pladser er lige. (2 eller 4). Da man ved at skrive Tavlens vertikale Række skrev Bogstaverne i alfabetisk Orden, idet man sprang hvert andet Felt over, kunne kun nogle faa Bogstaver komme 2 eller 4 Pladser over eller under et bestemt Bogstav, og dette kan altsaa i Depechen kun betegnes ved nogle ganske faa andre Bogstaver. Saaledes se vi, at der to Pladser under og over a overalt staaer ø og b med Undtagelse af to Steder (a- og ø-Rækken), hvor der staaer p og n. a i Depechen maa altsaa, hvis vi ere gaaede to Pladser over eller under, næsten altid betegne b eller ø, undtagelsesvis p eller n. Paa samme Maade betegner b sædvanlig c eller a, undtagelsesvis q eller o, og saaledes med dem alle. Er man gaaet 4 Pladser over eller under sit Bogstav, kan a betegne c eller æ, undtagelsesvis q eller m o. s. v. Man behøver derfor blot at danne sig en Tabel over de Bogstaver, som hvert enkelt Bogstav kan betegne, og man vælger da let dem, der give Mening, og læser saaledes Depechen uden Nøgle. Vi kunne ikke forud gjøre Forskjel paa under og over, fordi vi ikke vide, om Sedlen er brugt med det øverste eller det nederste Bogstav til Nøglebogstav. Er f. Ex. Depechen:

w p b u y – v l k l i – m m o k g – f,

prøve vi først, om man er gaaet 2 Pladser op eller ned, idet man under hvert Bogstav sætter de fire Bogstaver, som det kan betegne; vi faae da:

w	p	b	u	y
x	q	c	v	z					
v	o	a	t	x					
j	c	q	h	l					
h	a	o	f	z					

Man behøver ikke at gaa videre. w maatte snarest være v, p maatte da være o eller a, men man kan nu ikke finde Bogstaver for de næste, der kunne give

Mening; da det Samme gjælder om x, j eller h som første Bogstav, opgive vi denne Hypothese og undersøge, om Depechebogstavet er taget 4 Pladser over eller under det givne Bogstav. Under denne Forudsætning faae vi paa samme Maade:

w p b u y - v l k l i - m m o k g - f

y r d w æ v n m n k o o q m i h
u n ø s w t j i j g k k m i e d
k d r i m j o æ o y a a c æ w v
g ø n e i f x w x u y y æ w s r

hvor, som man erindrer, de to øverste Bogstaver have den overvejende Sandsynlighed for sig. Man seer nu ogsaa let, at man ved overalt at bruge et af disse (undtagen for f, der maa betegne r) faaer

U n d s æ t n i n g k o m m e r .

Det er saaledes altid let at løse en saadan Depeche uden Nøgle, men Nøglen selv findes kun, naar man har en længere Depeche. At w betegner u, viser kun, at det første Nøglebogstav ikke kan være et af de to, hvor w betegner k eller g (i og h). Det Eneste, der giver nogen videre Oplysning, er det Sidste, der viser, at det hertil svarende Nøglebogstav er d eller r.

Naar man paa denne Maade har undersøgt de Tilfælde, der ere mulige, naar Depechebogstavet er taget et lige Antal Pladser over eller under det givne Bogstav, og ikke har faaet nogen Kombination, der er Mening i, gaer man over til den anden Forudsætning, nemlig at

II. Antallet af Pladser er ulige. Dette Tilfælde er meget vanskeligere, da her et Bogstav kan betegnes ved alle de andre. Vi begynde da med en Undersøgelse, ganske som den, vi anvendte ved le carré indéchiffable, for at bestemme Antallet af Bogstaver i Nøglen og det Bogstav, der for hvert Nøglebogstav sandsynligvis betegner e. Vi søge herpaa de Steder, paa hvilke det bogstav, der betegner e, staaer 1, 3 eller 5 Pladser over e. Vi kunne nøjes med at tage Tilfældet „over” i Betragtning, naar vi ogsaa betragte Sedlerne i den omvendte Stilling da det her er over i det ene Tilfælde, bliver under i det andet. For Nemheds Skyld kunne vi een Gang for alle danne os en Hovednøgle, det vil sige en Tabel, der for hvert Bogstav viser os, paa hvilke Sedler det forekommer 1, 3 eller 5 Pladser over e. Denne Tabel faaer følgende Form:

[REDACTED]

	1.	2.	3.	4.	5.
1. Pl.	y;	b, k:	w, a;	n, c;	æ, a
2. Pl.	j;	o, z, s;	h, n;	a, p;	l, n
3. Pl.	z, s;	c, j, q;	x, b;	b, d;	ø, u, b.

I en af disse 6 Linier maa man nu kunne læse Nøgleordet. Man seer strax, at det først lykkes at danne et Ord af femte Linie, hvor der tydelig staaer Johan. Da desuden denne Linies Plads viser os, at Depechebogstaverne ere tagne tre Pladser under de givne Bogstaver, kunne vi nu let dechifrere Depechen og finde:

„Naar vi bruge den samme Form til at o. s. v.”

Dersom der er brugt en Nøgle, hvis Bogstaver ikke danne noget Ord, maa man dechifrere Stykker af Depechen med de forskellige mulige Nøgler, man har fundet, og man vil da træffe den, der giver mening, og kunne rette et eller andet Bogstav, der muligvis er valgt urigtigt. Man ledes da i Valget ved de andre hyppig forekommende Bogstaver. Dersom f.Ex. e i tredie Række af det andet Skema ikke var betegnet ved m, men ved y, maatte Nøglebogstavet være henholdsvis o, ø eller p, og m vilde da betegne:

q;	q;	q;
r	ø	v

af hvilke i alt Fald q og ø ere lidet sandsynlige. Derved kasseres fire af de mulige Nøgler, og ved paa samme Maade at benytte flere hyppig forekommende Bogstaver, faae vi det Antal, vi have at vælge imellem, meget formindsket.

Af de følgende to til vor Læses Skarpsindighed appellerende Depecher er man i den første gaaet et lige Antal Pladser (ikke over 6), i den anden et ulige Antal Pladser (ikke over 5) op eller ned. Antallet af Bogstaver i den sidste Nøgle er over 5 og under 10. I det andet Stykke af II er begyndt med Nøglen forfra.

I.

bgpht – æbumc – dnmæb – cgtku – givc.

II.

awymc – økvas – mmfly – yr1xl – tøivz – eyvfg – æhcty – mriæc –
 jsmus – ydect – ygshy – jzeyv – fuhut – vbigh – ucasz – uipsv – xemug –
 ldcas – pytæs – hævcem – ghueø – glyyø – seøfr – ziguh – yopyx – isvjs –
 zoømd – c.

ørkut – lrxef – yifzc – hntyw – bcebn – smusi – svssz – uvhgø –
øcunb –lgbxk – zughr – bdzwu – xisrg – fkuyø – sq.

Til Depechen i Nr. 152 var Nøglen “Haderslev” og Udtydningen saaledes:

Som bekjendt bliver Desdemona saavel i Shakespeares Tragedie som i Rossinis Opera muerdet af Negeren Othello; men hendes Gemal var ingen Neger, og Shakespeare tog fejl, dersom han troede det; det er hans Familienavn, der har foraarsaget Vildfarelsen.

Rigtige Løsninger ere indgaaede fra:

Asli; B. B.; E. Bj.; 326451; Touristen fra Hareskov; Marie ved Kirken; A. B-n; Pagaten.