En introduktion till några klassiska chiffer

Daniel Bosk*

krypto.tex 1674 2014-03-19 14:39:35Z danbos

Innehåll

1 Inledning

Ordet kryptografi kommer från grekiskans κρυπτός (*kryptos*) och γράφος (*graphos*) [2]. Dessa betyder *gömd* eller *hemlig* [1] respektive *skrift* [3]. Ordet kryptografi betyder följaktligen *hemlig skrift*.

Människan har troligtvis använt sig av kryptografi lika länge som skriftspråket har funnits, för om vi ser till människans historia har det mer eller mindre alltid funnits hemligheter. Kryptografin har då kunnat utvecklats under väldigt lång tid. Genom tiderna har det utvecklats många kryptoapparater, vi ska i denna text bland annat titta på en av de äldsta.

2 Terminologi för kryptosystem

När vi pratar om kryptografi används viss terminologi. Vi har en klartext och ett klartextalfabete. *Klartexten*[1] är det hemliga meddelande som vi vill skydda med hjälp av kryptografi. *Klartextalfabetet*[2] är det alfabete som används för att skriva klartexten.

Sedan har vi också en kryptotext och ett kryptoalfabete. *Kryptotext*[3] är den resulterande texten som vi får efter att vi krypterat vår klartext. *Kryptoalfabetet*[4] är det alfabete som används för kryptotexten.

I de kryptosystem som finns i denna text används olika delar av det vanliga alfabetet som klartextalfabete respektive kryptoalfabete. För att kunna skilja på vilket som är vilket väljer vi våra gemener för klartextalfabetet, exempelvis *abc...*, och våra versaler för kryptoalfabetet, exempelvis *ABC...*.

För att kunna kryptera och avkryptera krävs en *hemlig nyckel*[5], det är alltså nyckeln som ska hållas hemlig. För att kunna avkryptera ett hemligt meddelande, en kryptotext, krävs nyckeln. Med fel nyckel ger avkrypteringen bara en text med osammanhängande kombinationer av tecken från klartextalfabetet.

2.1 Formell definition av ett kryptosystem

Låt oss inleda med att definiera vad vi menar när vi skriver kryptosystem. Vi kommer i denna text att använda samma matematiska notation som Stinson [8].

Definition 1. Ett *kryptosystem* är en tupel $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ där följande gäller:

1. $\mathcal{P}$ är en ändlig mängd av möjliga klartexter.
2. $\mathcal{C}$ är en ändlig mängd av möjliga kryptotexter.
3. $\mathcal{K}$, kallad *nyckelrymden*, är en ändlig mängd av möjliga nycklar.
4. För varje $k \in \mathcal{K}$ finns en *krypteringsregel* $e_k \in \mathcal{E}$ och motsvarande *avkrypteringsregel* $d_k \in \mathcal{D}$. Varje $e_k \colon \mathcal{P} \to \mathcal{C}$ och $d_k \colon \mathcal{C} \to \mathcal{P}$ är funktioner sådana att $d_k(e_k(p)) = p$ för alla klartexter $p \in \mathcal{P}$.

[1] Engelskans *plaintext*.
[2] Engelskans *plaintext alphabet*.
[3] Engelskans *ciphertext*.
[4] Engelskans *ciphertext alphabet*.
[5] Engelskans *secret key*.

Figur 1: En skytale där texten ”KEISER AUGUSTIN . . . ” skrivits. Bild: Wikipedia [9].

Det är den sistnämda egenskapen som gör att vi kan kommunicera utan tvetydigheter. Samma egenskap säger också att det är nyckeln k som måste hållas hemlig för att vår kommunikation ska hållas säker.

3 Skytale

En av de tidigare uppfinningarna som kunnat tillämpas inom kryptografin var ett redskap som heter *skytale*. Den bestod av en pinne av en given tjocklek och en läderrem. Läderremmen lindades runt pinnen, och därefter skrevs det hemliga meddelandet på remmen. Se bild i figur 1. När meddelandet var klart lindades läderremmen av från pinnen och den fördes till mottagaren. För att kunna läsa texten på läderremmen krävdes att läsaren lindade upp remmen på en pinne av samma tjocklek som användes vid skapandet av meddelandet. Om en pinne av fel diameter används kommer bokstäverna att hamna fel och texten blir oläsbar.

Det är dock omdebatterat huruvida denna ”kryptoapparat” uppfanns med syfte att vara en kryptoapparat eller bara en metod att lagra meddelanden eller en metod att verifiera avsändare [5]. Hur det än är kan den tillämpas på sådant sätt att det blir ett chiffer, och det chiffret tittar vi på här.

Det chiffer som används i kryptoapparaten skytale kan generaliseras enligt följande. Först bestäms bredd och höjd för en rektangel av rutor, där en bokstav ska skrivas i varje ruta. Därefter skrivs texten radvis i rutorna i rektangeln. Då kan den krypterade texten läsas kolumnvis istället för radvis.

Exempel 1. Vi vill kryptera texten *En dag i juni*. Vi använder radbredden 7 och kolumnhöjden 2 och markerar tomma rutor med en punkt. Vi får då

```
en_dag_
i_juni.
```

Kryptotexten blir då *EIN__JDUANGI_*.. För att avkryptera skriver vi bara texten i samma rektangel.

```
EN_DAG_
I_JUNI.
```

Om vi vill skriva ett längre meddelande används flera rutor.

Denna typ av chiffer kallas för *transpositions-* eller *permutationschiffer*[6].

[6]Engelskans *transposition cipher* eller *permutation cipher*.

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$\pi(i)$	1	8	2	9	3	10	4	11	5	12	6	13	7	14

Tabell 1: Definitionen av permutationen π.

3.1 Formell definition av permutationschiffer

Formellt definierar vi ett permutationschiffer enligt följande.

Definition 2 (Permutationschiffer)**.** Låt n vara ett positivt heltal och A ett alfabet. Låt också $\mathcal{P} = \mathcal{C} = A^n$ och låt $\mathcal{K}$ vara alla möjliga permutationer av mängden $\{1, \ldots, n\}$. För en permutation $\pi \in \mathcal{K}$ definierar vi

$$e_\pi(p_1, \ldots, p_n) = (p_{\pi(1)}, \ldots, p_{\pi(n)}),$$

för alla klartexter $p = (p_1, \ldots, p_n) \in \mathcal{P}$, och

$$d_\pi(c_1, \ldots, c_n) = (c_{\pi^{-1}(1)}, \ldots, c_{\pi^{-1}(n)}),$$

för alla kryptotexter $c = (c_1, \ldots, c_n) \in \mathcal{C}$ och där π^{-1} är den inverterade permutationen π.

Låt oss illustrera definitionen genom att tillämpa den på exempel 1.

Exempel 2. Låt $n = 7 \times 2 = 14$. Vi låter också permutationen $\pi \in \mathcal{K}$ definieras enligt tabell 1. För att kryptera använder vi $e_\pi \in \mathcal{E}$. Om vi låter $p = (p_1, \ldots, p_n)$ vara vår klartext ”en dag i juni”, alltså $p_1 = e, p_2 = n$ och så vidare, får vi att $c = e_\pi(p) = (p_1, p_8, p_2, p_9, \ldots, p_7, p_{14})$ och således att c är vår kryptotext ”EIN_ _JDUANGI_.”.

Vi avkrypterar på samma sätt med hjälp av π^{-1}.

Vi ser också ganska omedelbart att antalet möjliga nycklar $|\mathcal{K}| = n!$ växer snabbt med antalet bokstäver n i ett block som permuteras.

4 Caesarchiffer

Chiffret vi ska titta på i detta avsnitt är uppkallat efter den romerske diktatorn och kejsaren Julius Caesar (49 f.Kr. – 44 e.Kr.). Även om chiffret troligtvis uppfunnits tidigare har det fått detta namn eftersom att Caesar lär ha använt det med nyckeln given i tabell 2 [8]. Chiffret är annars även känt som ett skiftchiffer, vi kommer att se varför.

Chiffret använder det vanliga alfabetet som både klartext- och kryptoalfabete. För att kryptera förskjuts kryptoalfabetet mot klartextalfabetet ett givet antal steg. Det är antalet steg som utgör nyckeln i Caesarchiffret. Därefter krypteras meddelandet genom att varje klartextbokstav motsvaras av en kryptotextbokstav. Se tabell 2.

Exempel 3. För att kryptera klartexten *hej* slår man upp bokstav för bokstav i tabell 2. Det vill säga, $h \mapsto J$, $e \mapsto G$ och $j \mapsto L$. Kryptotexten blir alltså *JGL*.

Exempel 4. Om vi krypterar ordet *skatten* blir det *UMCVVGP*.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
p	q	r	s	t	u	v	w	x	y	z	å	ä	ö	
R	S	T	U	V	W	X	Y	Z	Å	Ä	Ö	A	B	

Tabell 2: Tabell för att kryptera med ett Caesarchiffer med nyckeln C.

4.1 Formell definition av Caesarchiffret

Låt oss ge följande definition av Caesar- eller skiftchiffret.

Definition 3 (Skiftchiffer)**.** Låt $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{29}$ och låt varje bokstav i det svenska alfabetet motsvara ett unikt tal i $\mathbb{Z}_{29}$. För alla $k \in \mathcal{K}$ definierar vi

$$\begin{aligned} e_k(p) &= (p + k) \bmod 29, \text{ och} \\ d_k(c) &= (c - k) \bmod 29, \end{aligned}$$

där $p \in \mathcal{P}$ är en klartextbokstav och $c = e_k(p) \in \mathcal{C}$ är motsvarande kryptotext-bokstav.

Vi förtydligar definitionen med ett exempel.

Exempel 5. Låt oss numrera bokstäverna i det svenska alfabetet enligt index med start från noll. Då får vi att textsträngen ”hej” skulle kunna motsvaras av tupeln $p = (7, 4, 9)$. Om vi låter nyckeln $k \in \mathcal{K}$ vara 2 får vi att

$$\begin{aligned} c = e_2(p) &= (e_2(7), e_2(4), e_2(9)) \\ &= (9, 6, 11). \end{aligned}$$

Om vi översätter tillbaka till bokstäver får vi att c motsvarar strängen ”JGL”.

Vi ser här att antalet möjliga nycklar $|\,\mathcal{K}\,| = |\,\mathbb{Z}_{29}\,| = 29$ är alldeles för få.

4.2 Kryptanalys av Caesarchiffret

Caesarchiffret är inte ett särskilt säkert sätt att skydda information. Det är lätt att knäcka. Det finns totalt, om det svenska alfabetet används, 29 olika nycklar som kan användas för kryptering och avkryptering eftersom att alfabetet maximalt kan förskjutas lika många steg som det finns bokstäver[7]. Detta är så få att det till och med enkelt kan testas för hand för att lista ut vilken nyckel som använts. Om det finns tillgång till en dator och man kan programmera, då är det ännu enklare. Men det går tack vare språkets egenskaper att reducera antalet nycklar som behöver testas ytterligare. Titta på exempel 4 där *tt* blir *VV*, det är långt från alla bokstäver i svenskan som upprepas på detta sätt. I avsnitt 5.2 ska vi se ytterligare ett sätt att kryptanalysera Caesarchiffret på.

[7]Detta kan beräknas genom att vi på den första platsen kan välja mellan 29 bokstäver, på de efterföljande platserna kan då bara välja en bokstav. Vi får då totala antalet nycklar genom $29 \cdot 1 \cdot 1 \cdots 1 = 29$.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
C	M	Q	F	Z	Ö	I	J	P	L	D	N	O	K	D
p	q	r	s	t	u	v	w	x	y	z	å	ä	ö	
R	S	T	Å	V	Y	X	W	G	U	Ä	H	A	B	

Tabell 3: Tabell för att kryptera med ett substitutionschiffer. Gemener används som klartextalfabete och versaler som kryptoalfabete.

5 Substitutionschiffer

I ett *substitutionschiffer* avbildas varje bokstav i klartextalfabetet på en unik bokstav i kryptoalfabetet. Caesarchiffret är alltså ett substitutionschiffer. I dagstidningar, bland korsorden, brukar det finnas en typ av korsord som kallas för krypto, där rutorna är markerade med tal och varje tal motsvarar en bokstav. Här används alltså det vanliga alfabetet, $a, b, c, \cdots$, som klartextalfabete och talen $1, 2, 3, \cdots, 29$ som kryptoalfabete. Nyckeln i substitutionschiffret utgör hela avbildningen mellan klartext- och kryptoalfabetet. Ett exempel visas i tabell 3.

För att kryptera gör man på samma sätt som i Caesarchiffret.

Exempel 6. För att kryptera klartexten *hej* slår man upp bokstav för bokstav i tabell 3. Det vill säga, $h \mapsto J$, $e \mapsto Z$ och $j \mapsto L$. Kryptotexten blir alltså *JZL*.

Exempel 7. Om vi krypterar ordet *skatten* blir det *ÅDCVVZK*.

5.1 Formell definition av substitutionsciffer

Vi definierar substitutionschiffret som följer. För enkelthet använder vi samma alfabet för både klartext och kryptotext, även om detta inte är en nödvändig begränsning. Om vi vill ha ett annat kryptoalfabet är detta egentligen bara en fråga om kodning, och detta kan läggas till i efterhand.

Definition 4 (Substitutionschiffer)**.** Låt A vara vårt alfabet och låt $\mathcal{P} = \mathcal{C} = A$. Vidare låt $\mathcal{K}$ bestå av alla möjliga permutationer av A. För varje permutation $\pi \in \mathcal{K}$ definierar vi att

$$e_\pi(p) = \pi(p), \text{ och}$$
$$d_\pi(c) = \pi^{-1}(c),$$

där π^{-1} är den inverterade permutationen π, $p \in \mathcal{P}$ är en klartextbokstav och $c = e_\pi(p) \in \mathcal{C}$ är motsvarande kryptotextbokstav.

Notera skillnaden mellan användningen av permutationen π i denna definition och den i definition 2. I den tidigare användes permutationen på index i ett block medan i denna definition används permutationen direkt på enskilda tecken. Här permuteras bokstaven medan i den tidigare permuterades bokstavens position.

Vi förtydligar definitionen med följande exempel.

Exempel 8. Vi kan här återanvända exempel 6. Vi låter A vara det svenska alfabetet. Nyckeln $\pi \in \mathcal{K}$ kan vi låta vara densamma som i exempel 6, vilken vi ser i tabell 3. Då får vi att $e_\pi(h) = J, e_\pi(e) = Z, e_\pi(j) = L$.

α	a	b	c	d	e	f	g	h	i	j
$\Pr(X = \alpha)$	0.063	0.000	0.000	0.031	0.156	0.000	0.031	0.094	0.064	0.000
α	k	l	m	n	o	p	q	r	s	t
$\Pr(X = \alpha)$	0.000	0.063	0.000	0.094	0.031	0.000	0.000	0.031	0.156	0.125
α	u	v	w	x	y	z	å	ä	ö	
$\Pr(X = \alpha)$	0.000	0.000	0.031	0.031	0.000	0.000	0.000	0.000	0.000	

Tabell 4: Tabell av sannolikhetsfördelningen för den stokastiska variabeln X som antar bokstäver i meningen "anenglishtexthasnoswedishletters", angiven med tre decimalers noggrannhet.

Värt att notera är att antalet möjliga nycklar $|\mathcal{K}| = |A|!$ växer snabbt med storleken av alfabetet.

5.2 Kryptanalys av substitutionschiffer

För generella substitutionschiffer finns det väsentligen fler möjliga nycklar än de 29 möjligheter som fanns för Caesarchiffret, men till kostnad av en längre nyckel som är svårare att memorera. Som första bokstav i nyckeln kan vi välja mellan alla 29 bokstäverna i alfabetet. För varje bokstav vi kan välja som första bokstav finns det 28 bokstäver kvar som då kan välja mellan. Vi får således

$$29! = 29 \cdot 28 \cdot 27 \cdots 3 \cdot 2 \cdot 1 = 8841761993739701954543616000000$$

möjliga nycklar[8], vilket gör det svårt att testa alla möjliga nycklar som vi kunde göra med Caesarchiffret. Vi behöver alltså en annan metod.

Vi analyserar följande text: "An English text has no Swedish letters". Vi vill nu beräkna sannolikheten att välja en specifik bokstav om vi väljer en slumpmässig bokstav i denna mening. Det vill säga, vi väljer en slumpmässig bokstav från mängden

$$A = \{a, n, e, g, l, i, s, h, t, x, o, w, d, r\}.$$

Låt X beteckna en stockastisk variabel som antar värden ur A. Vi vet från sannolikhetsläran att sannolikheten $\Pr(X = a)$ att vi väljer a och att detta värde beräknas som

$$\Pr(X = \alpha) = \frac{\#\alpha}{N},$$

där $\#\alpha$ är antalet förkomster av α i texten och N är totala antalet tecken i texten. Vi kan då beräkna att $\Pr(X = a) = 0.0625$ och alltså att sannolikheten att en slumpvis vald bokstav i texten är ett a är 6.25 procent. Värdena av $\Pr(X = \alpha)$ för samtliga värden av α ges i tabell 4.

Om vi krypterar en text med ett substitutionschiffer, exempelvis ett Caesarchiffer, då förändrar vi inte antalet av någon bokstav, det enda vi ändrar är bokstavens representation ("utseende"). Vi krypterar "anenglishtexthasnoswedishletters" med något okänt substitutionschiffer och får då

CPGPINKUJVGZVJCUPQUYGFKUJNGVVGTU.

[8] 29! uttalas *29 fakultet*.

α	A	B	C	D	E	F	G	H	I	J
$\Pr(Y = \alpha)$	0.000	0.000	0.063	0.000	0.000	0.031	0.156	0.000	0.031	0.094
α	K	L	M	N	O	P	Q	R	S	T
$\Pr(Y = \alpha)$	0.064	0.000	0.000	0.063	0.000	0.094	0.031	0.000	0.000	0.031
α	U	V	W	X	Y	Z	Å	Ä	Ö	
$\Pr(Y = \alpha)$	0.156	0.125	0.000	0.000	0.031	0.031	0.000	0.000	0.000	

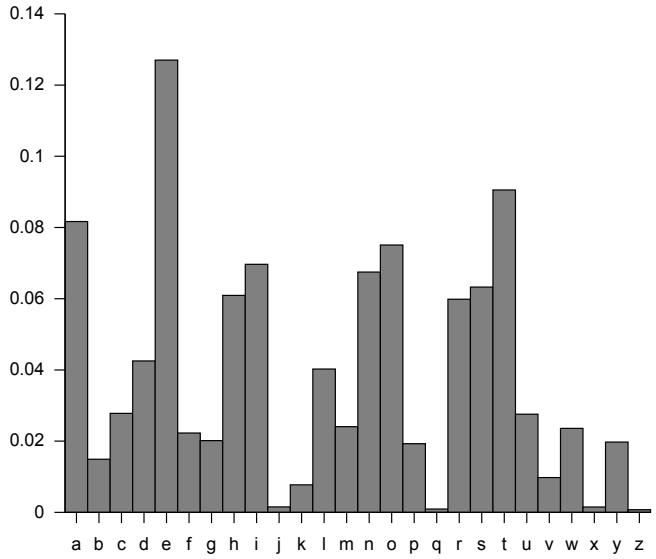
Tabell 5: Tabell av sannolikhetsfördelningen för den stokastiska variabeln Y som antar bokstäver i meningen ”CPGPINKUJVGZVJCUPQUYGFKUJNGVVGTU”, angiven med tre decimalers noggrannhet.

α	a	b	c	d	e	f	g	h	i	j
$\Pr(E = \alpha)$	0.082	0.015	0.028	0.043	0.127	0.022	0.020	0.061	0.070	0.002
$\Pr(S = \alpha)$	0.093	0.013	0.013	0.045	0.099	0.020	0.033	0.021	0.051	0.007
α	k	l	m	n	o	p	q	r	s	t
$\Pr(E = \alpha)$	0.008	0.040	0.024	0.067	0.075	0.019	0.001	0.060	0.063	0.091
$\Pr(S = \alpha)$	0.032	0.052	0.035	0.088	0.041	0.017	0.000	0.083	0.063	0.087
α	u	v	w	x	y	z	å	ä	ö	
$\Pr(E = \alpha)$	0.028	0.010	0.023	0.001	0.020	0.001	0.000	0.000	0.000	
$\Pr(S = \alpha)$	0.018	0.024	0.000	0.001	0.006	0.000	0.016	0.021	0.015	

Tabell 6: Tabell av sannolikhetsfördelningen för bokstäver i det engelska [8] och det svenska [10] språket, den stokastiska variabeln E respektive S, angiven med tre decimalers noggrannhet.

Vi låter den stokastiska variabeln Y anta bokstäver i meningen ovan. Sannolikhetsfördelningen för Y är tabellerad i tabell 5. Om vi tittar i tabellen ser vi att $\Pr(X = a) = \Pr(Y = C) = \Pr(Y = N)$, då har vi alltså två alternativ som skulle kunna representera a i kryptoalfabetet. Ett bra riktmärke kan vara att titta på den vanligaste bokstaven, i klartextalfabetet är det e med $\Pr(X = e) = 0.156$. Det är då mycket möjligt att $e \mapsto G$ eftersom att $\Pr(Y = G)$ också är 0.156. Ytterligare information vi kan använda är återupprepningar hos bokstäver, jämför med exempel 4 och 7 där t:et i ordet *skatten* upprepar sig. De enda bokstäver som upprepar sig i svenskan är konsonanter, och bokstäverna omkring dessa är oftast vokaler. Av vad vi sett hittills verkar det som att kryptotexten är krypterad med ett Caesarchiffer med nyckeln C eftersom att $a \mapsto C$ och $e \mapsto G$ är troliga avbildningar. Om vi testar att avkryptera enligt Caesarchiffret med nyckeln C ser vi att vår gissning var korrekt.

Nu kände vi till sannolikhetsfunktionen för klartexten när vi tittade på kryptotexten, men hur gör man egentligen när man inte vet någonting om klartexten? Om man har tillräckligt mycket text kommer sannolikhetsfunktionen för texten att närma sig sannolikhetsfunktionen för språket. Då kan textens sannolikhetsfunktion jämföras för att först se vilket språk texten är skriven på och därefter kan man hitta nyckeln som vi gjorde ovan. Sannolikhetsfunktionen för språken svenska och engelska finns givna i tabell 6. En överblicksbild för det engelska språket ges även i figur 2. Sannolikhetstabeller för några olika språk finns tillgängliga hos Wikipedia [10].



Figur 2: En överblickande graf över sannolikhetsfördelningen för den stokastiska variabeln E. Bild: Wikipedia [10].

Övning 1. Du jobbar som kryptoanalytiker åt Försvarets Radioanstalt (FRA) och får följande text på ditt skrivbord:

```
VJGOCFJCVVGTUVGCRCTVUWPFGTYC
KVKUKPVJGWUWCNRNCEGDGJKPFVJGEWTVCKP
```

Vad betyder det?

6 Vigenèrechiffer

Grunden för Vigenèrechiffret lades under 1400-talet av Leon Battista Alberti (1404–1472) [7]. Därefter vidareutvecklades hans idéer först av Johannes Trithemius (1462–1516) och sedan av Giambattista della Porta (1535–1615) [7]. Anledningen till att metoden kallas Vigenèrechiffer är för att den är uppkallad efter Blaise de Vigenère (1523–1596) som gjorde det slutgiltiga bidraget till utformningen av chiffret [7]. Vigenèrechiffret användes länge, det användes till och med av sydstaterna under det amerikanska inbördeskriget.

Chiffret består av upprepad användning av Caesarchiffret. Som nyckel används ett ord, för att vara enkelt att komma ihåg, vilket bokstavskombination som helst kan användas. Vid kryptering av en text krypteras första bokstaven i klartexten med ett Caesarchiffer där första bokstaven i Vigenèrenyckeln används som nyckel. Därefter används den andra, den tredje, och så vidare. När nyckelordets alla bokstäver använts börjar man om.

Exempel 9. Om vi vill kryptera order *skatten* ska bokstäverna i nyckeln användas enligt

```
skatten
ABCABCA
```

Klartext	a	b	c	d	e	f	g	h	i	j
A	A	B	C	D	E	F	G	H	I	J
B	B	C	D	E	F	G	H	I	J	K
C	C	D	E	F	G	H	I	J	K	L
Klartext	k	l	m	n	o	p	q	r	s	t
A	K	L	M	N	O	P	Q	R	S	T
B	L	M	N	O	P	Q	R	S	T	U
C	M	N	O	P	Q	R	S	T	U	V
Klartext	u	v	w	x	y	z	å	ä	ö	
A	U	V	W	X	Y	Z	Å	Ä	Ö	
B	V	W	X	Y	Z	Å	Ä	Ö	A	
C	W	X	Y	Z	Å	Ä	Ö	A	B	

Tabell 7: Vigenèrechiffer med nyckeln *ABC*.

och vi får alltså *SLCTUGN* genom att använda de olika Caesarchiffren i tabell 7.

Notera skillnaden mellan kryptotexten av ordet *skatten* i exempel 4, exempel 7 och exempel 9. Upprepningen av t:et försvinner när Vigenerechiffret används.

6.1 Formell definition av Vigenèrechiffret

Vi går vidare med en definition av Vigenèrechiffret.

Definition 5 (Vigenèrechiffer)**.** Låt n vara ett positivt heltal. Definiera att $\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_{29})^n$. För alla nycklar $k = (k_1, \ldots, k_n) \in \mathcal{K}$, klartexter $p = (p_1, \ldots, p_n) \in \mathcal{P}$ och kryptotexter $c = (c_1, \ldots, c_n) \in \mathcal{C}$ definierar vi att

$$e_k(p) = (p_1 + k_1, \ldots, p_n + k_n), \text{ och}$$
$$d_k(c) = (c_1 - k_1, \ldots, c_n - k_n),$$

där alla operationer utförs i $\mathbb{Z}_{29}$.

Vi noterar att den enda skillnaden mellan denna definition och definition 3 är att $\mathcal{P}, \mathcal{C}, \mathcal{K}$ definieras som $(\mathbb{Z}_{29})^n$ istället för $\mathbb{Z}_{29}$. Låter vi $n = 1$ är dessa system identiska.

Om vi använder gruppen $\mathbb{Z}_2$ istället för $\mathbb{Z}_{29}$ kommer vi att arbeta med bitsträngar av längden n bitar. Detta får effekten att $e_k(p) = p \oplus k$ där p och k är bitstängar av längd n, det vill säga operationen *bitvis exklusivt eller* (XOR). Detta är en fundamental operation i dagens datorer.

6.2 Kryptanalys av Vigenèrechiffret

Eftersom att kryptotexten nu är krypterad med flera Caesarnycklar fungerar inte längre metoden som vi tog fram i avsnitt 5.2. Friedrich Kasiski (1805–1881) publicerade år 1863 tekniken hur man fullständigt knäcker chiffret utan några förkunskaper [8]. Tidigare metoder, före Kasiski, krävde att man kände till delar av klartexten, att man kunde gissa nyckeln eller kände nyckelns längd.

Med mycket kryptotext är det möjligt att finna upprepningar i kryptotexten. Avståndet mellan upprepningarna måste vara en multipel av nyckelns längd eftersom att samma klartext annars skulle krypteras olika på grund av att olika delar av nyckeln används. Det vill säga, nyckelns längd måste vara en gemensam faktor för alla avstånd mellan upprepningar. Om vi tittar på följande exempel.

Exempel 10. Ett Vigenèrechiffer med nyckeln *ABCD* används för att kryptera texten *cryptoisshortforcryptography*.

```
Nyckel:     ABCDABCDABCDABCDABCDABCDABCD
Klartext:   cryptoisshortforcryptography
Kryptotext: CSASTPKVSIQUTGQUCSASTPIUAQJB
```

Avståndet mellan den upprepade texten *CSASTP* är 16, från första tecken till första tecken. De möjliga nyckellängderna är alltså $16, 8, 4, 2$ eller 1.

Genom att finna flera sådana upprepningar är det möjligt att reducera antalet möjliga nyckellängder.

När nyckellängden väl är känd, låt oss säga att den är n tecken, då skrivs kryptotexten med n teckens bredd. Som vi ser i exempel 10 hamnar då alla tecken krypterade med samma Caesarnyckel ovanför varandra i en kolumn, se exempel 11.

Exempel 11. Ett Vigenèrechiffer med nyckeln *ABCD* används för att kryptera texten *cryptoisshortforcryptography*.

```
Nyckel:     ABCD
Klartext:   cryp
            tois
            shor
            tfor
            cryp
            togr
            aphy
Kryptotext: CSAS
            TPKV
            SIQU
            TGQU
            CSAS
            TPIU
            AQJB
```

Eftersom att varje kolumn nu är krypterad endast med ett Caesarchiffer kan vi enkelt använda kryptanalysmetoderna från avsnitt 4.2 eller avsnitt 5.2 för att lista ut varje Caesarnyckel och därmed hela Vigenèrenyckeln. I exempel 11 analyserar vi den första kolumnen för att komma fram till att den är krypterad med nyckeln *A*, den andra kolumnen är krypterad med nyckeln *B*, och så vidare, och slutligen att Vigenèrechiffrets nyckel är *ABCD*.

7 Engångschiffer och perfekt sekretess

Vi inleder detta avsnitt med att definiera vad vi menar med perfekt sekretess[9]. Detta begrepp publicerades första gången av Shannon [6] år 1949.

Definition 6. Ett kryptosystem $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ sägs ha *perfekt sekretess* om $\Pr(P = p \mid C = c) = \Pr(P = p)$ för alla $p \in \mathcal{P}$ och $c \in \mathcal{C}$. Det vill säga, sannolikheten a posteriori att en klartext är p om kryptotexten är c är densamma som sannolikheten a priori att klartexten är p.

Låt oss fortsätta med att visa några resultat om perfekt sekretess. Vi inleder med följande lemma som fastställer för en typ av kryptosystem några egenskaper som krävs för att detta system ska tillhandahålla perfekt sekretess.

Lemma 1. *Låt $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ vara ett kryptosystem. Om $|\mathcal{K}| = |\mathcal{C}| = |\mathcal{P}|$ och varje nyckel används med sannolikheten $1/|\mathcal{K}|$ och det för varje klartext $p \in \mathcal{P}$ och kryptotext $c \in \mathcal{C}$ finns en unik nyckel $k \in \mathcal{K}$ sådan att $e_k(p) = c$, då tillhandahåller kryptosystemet perfekt sekretess.*

Bevis. Antag $|\mathcal{K}| = |\mathcal{C}| = |\mathcal{P}|$. Vidare antag $\Pr(K = k) = 1/|\mathcal{K}|$ för alla nycklar $k \in \mathcal{K}$ och att det för alla klartexter $p \in \mathcal{P}$ och kryptotexter $c \in \mathcal{C}$ finns en nyckel $k \in \mathcal{K}$ sådan att $e_k(p) = c$ och för alla nycklar $k' \neq k$ gäller att $e_{k'}(x) \neq c$.

Låt $c \in \mathcal{C}$ vara en godtycklig kryptotext. Då har vi att

$$\Pr(C = c) = \sum_{k \in \mathcal{K}} \Pr(K = k) \Pr(P = d_k(c)).$$

Eftersom att $\Pr(K = k) = 1/|\mathcal{K}|$ för alla möjliga $k \in \mathcal{K}$ och att nyckeln är unik för varje klartext–kryptotextpar har vi

$$\begin{aligned} \Pr(C = c) &= \sum_{k \in \mathcal{K}} \frac{1}{|\mathcal{K}|} \Pr(P = d_k(c)) \\ &= \frac{1}{|\mathcal{K}|} \sum_{k \in \mathcal{K}} \Pr(P = d_k(c)). \end{aligned}$$

För en fixerad kryptotext $c \in \mathcal{C}$ är $d_k(c)$ en permutation av $\mathcal{P}$. Följaktligen får vi

$$\begin{aligned} \Pr(C = c) &= \frac{1}{|\mathcal{K}|} \sum_{p \in \mathcal{P}} \Pr(P = p) \\ &= \frac{1}{|\mathcal{K}|} \times 1 = \frac{1}{|\mathcal{K}|}. \end{aligned}$$

Vidare har vi att $\Pr(C = c \mid P = p) = \Pr(K = k)$ tack vare att det är en unik nyckel $k \in \mathcal{K}$ för varje par av klartext $p \in \mathcal{P}$ och kryptotext $c \in \mathcal{C}$.

Slutligen får vi då genom Bayes sats att

$$\begin{aligned} \Pr(P = p \mid C = c) &= \frac{\Pr(P = p) \Pr(C = c \mid P = p)}{\Pr(C = c)} \\ &= \frac{\Pr(P = p) \frac{1}{|\mathcal{K}|}}{\frac{1}{|\mathcal{K}|}} = \Pr(P = p). \end{aligned}$$

Då $\Pr(P = p \mid C = c) = \Pr(P = p)$ har vi perfekt sekretess. Q.E.D.

[9] Engelskans *perfect secrecy*.

Vi fortsätter med ett mer generellt resultat som visar att kryptosystem av denna typ som uppfyller perfekt sekretess måste uppfylla dessa egenskaper.

Sats 1 (Shannons sats)**.** *Antag att* $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ *är ett kryptosystem sådant att* $|\mathcal{K}| = |\mathcal{C}| = |\mathcal{P}|$*. Detta kryptosystem tillhandahåller perfekt sekretess om och endast om varje nyckel* $k \in \mathcal{K}$ *används med lika sannolikhet* $1/|\mathcal{K}|$ *och det för varje klartext* $p \in \mathcal{P}$ *och kryptotext* $c \in \mathcal{C}$ *finns en unik nyckel* $k \in \mathcal{K}$ *sådan att* $e_k(p) = c$*.*

Bevis. Vi har redan enligt lemma 1 att ett kryptosystem med dessa egenskaper ger perfekt sekretess. Det som återstår att visa är att ett system som uppfyller perfekt sekretess måste vara ett sådant system.

Låt oss därför anta $|\mathcal{K}| = |\mathcal{C}| = |\mathcal{P}|$ och att detta kryptosystem ger perfekt sekretess, det vill säga $\Pr(P = p \mid C = c) = \Pr(P = p)$. Från definitionen av kryptosystem (definition 1) har vi att för alla klartexter $p \in \mathcal{P}$ och kryptotexter $c \in \mathcal{C}$ existerar åtminstone en nyckel $k \in \mathcal{K}$ sådan att $e_k(p) = c$, det vill säga

$$|\mathcal{C}| = |\{e_k(p) \colon k \in \mathcal{K}\}| \leq |\mathcal{K}|.$$

Men enligt vårt antagande om typen av system är $|\mathcal{C}| = |\mathcal{K}|$, alltså kan det inte finnas två nycklar $k \in \mathcal{K}$ och $k' \in \mathcal{K}$ sådana att $k \neq k'$ och $e_k(p) = c$.

Vidare fixera en kryptotext $c \in \mathcal{C}$, låt $\mathcal{P} = \{p_i \colon 1 \leq i \leq n\}$ där $n = |\mathcal{K}| = |\mathcal{P}|$ och indexera nycklarna $k_i \in \mathcal{K}$ sådana att $e_{k_i}(p_i) = c$, för $1 \leq i \leq n$. Genom Bayes sats har vi då

$$\begin{aligned}\Pr(P = p_i \mid C = c) &= \frac{\Pr(P = p_i)\Pr(C = c \mid P = p_i)}{\Pr(C = c)} \\ &= \frac{\Pr(P = p_i)\Pr(K = k_i)}{\Pr(C = c)}.\end{aligned}$$

Eftersom att vi har perfekt sekretess $\Pr(P = p_i \mid C = c)$ får vi att

$$\frac{\Pr(P = p_i)\Pr(K = k_i)}{\Pr(C = c)} = \Pr(P = p_i).$$

och således att $\Pr(K = k_i) = \Pr(C = c)$. Då vi valt ett godtyckligt c måste K ha ett likformigt sannolikhetsmått. Följaktligen måste $\Pr(K = k_i) = 1/|\mathcal{K}|$ för alla nyklar $k_i \in \mathcal{K}$. Q.E.D.

Det sats 1 säger är att om vi använder ett Vigenèrechiffer, eller motsvarande kryptosystem, med en nyckel som är lika lång som klartexten och aldrig någonsin återanvänder nyckeln, då kommer kryptotexten att vara oknäckbar. Låt oss även ge en mer intuitiv förklaring. Säg att vi har krypterat klartexten $p \in \mathcal{P}$ med nyckeln $k \in \mathcal{K}$ och fått kryptotexten $c \in \mathcal{C}$. Angriparen kan då för varje möjlig klartext $p' \in \mathcal{P}$ hitta en nyckel $k' \in \mathcal{K}$ sådan att $e_{k'}(p') = c$. Det kommer följaktligen vara omöjligt att avgöra om p' eller p är den riktiga klartexten utan att ha mer information, båda klartexterna kommer att ha lika sannolikhet.

I exempel 11 kunde vi knäcka chiffret eftersom att nyckellängden var fyra medan längden av klartexten var sju gånger längre. Antalet möjliga nycklar $|\mathcal{K}|$ var alltså inte detsamma som antalet möjliga klartexter $|\mathcal{P}|$, följaktligen gick det enligt sats 1 ej att uppnå perfekt sekretess i det fallet.

Övning 2. Formulera en sats med bevis som bestämmer vad gäller perfekt sekretess för substitutionschiffer (definition 4), där $|\mathcal{P}| = |\mathcal{C}| \neq |\mathcal{K}|$.

Övning 3. Detsamma gäller permutationschiffer (definition 2), formulera en sats med bevis gällandes perfekt sekretess för detta chiffer.

Övning 4. Går det att dra någon generellt slutsats vad gäller perfekt sekretess för kryptosystem där $|\mathcal{P}| = |\mathcal{C}| \neq |\mathcal{K}|$? Bevisa denna slutsats eller visa att ingen sådan kan dras.

7.1 Vernams engångschiffer

Faktum är att redan år 1917 hade Gilbert Vernam beskrivit ett chiffer med egenskaperna som krävs i sats 1 [8], det vill säga långt innan Shannon hade publicerat teorin för att matematiskt visa perfekt sekretess. Detta engångschiffer, mer känt som *One-time Pad* (OTP), ges i följande definition.

Definition 7 (One-time Pad)**.** Låt n vara ett positivt heltal. Definiera att $\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_2)^n$. För alla nycklar $k = (k_1, \ldots, k_n) \in \mathcal{K}$, klartexter $p = (p_1, \ldots, p_n) \in \mathcal{P}$ och kryptotexter $c = (c_1, \ldots, c_n) \in \mathcal{C}$ definierar vi att

$$e_k(p) = (p_1 + k_1, \ldots, p_n + k_n),$$

där alla operationer utförs i $\mathbb{Z}_2$, och därefter definierar vi att $d_k = e_k$.

Nyckeln $k \in \mathcal{K}$ måste väljas slumpmässigt och får aldrig återanvändas.

Detta är ekvivalent med att arbeta med n bitar långa bitsträngar och där $e_k(p) = p \oplus k$ och $d_k(c) = c \oplus k$, den binära operationen $\oplus$ är *bitvis exklusivt eller* (XOR).

Övning 5. Låt $p, p' \in \mathcal{P}$ vara två klartexter och låt $k \in \mathcal{K}$ vara en kryptonyckel för OTP. Om vi krypterar de båda klartexterna med samma nyckel, $e_k(p)$ och $e_k(p')$, visa en attack som tar bort beroendet av nyckeln.

8 Moderna kryptosystem

Moderna kryptosystem är helt och hållet baserade på matematik, exempelvis resultat inom talteori och abstrakt algebra. De används dessutom till fler saker än att bara hålla information hemlig. Dagens kryptografi handlar också om att informationen ska kunna verifieras, för att se att ingen har ändrat på ett meddelande, och att se om det är rätt avsändare av meddelandet. Denna typ av kryptografi kallas *public key cryptography* eller *asymmetrisk kryptering*. Alla chiffer som diskuterats i föregående avsnitt är av typen *symmetrisk kryptering* där samma nyckel används för både kryptering och avkryptering. I asymmetrisk kryptering används alltså olika nycklar för kryptering och avkryptering.

Mycket av dagens kryptografi används i mobiltelefoner och datorer. Samtalet är krypterat från mobiltelefonen till basstationen, det vill säga under den sträcka det färdas genom luften som radiovågor. Anslutningen till en webbserver är krypterad när inloggningsuppgifter skickas till servern, exempelvis när man loggar in till sitt e-postkonto. Kryptografi används även för att verifiera att det är rätt webbserver som man kommunicerar med, för att undvika att skicka uppgifter till någon som låtsas vara rätt server. Det är därför viktigt att se i

webbläsaren så att det inte är en falsk server som man anslutit till. Detta visas i webbläsaren på olika otydliga vis, beroende på webbläsare, men de har blivit tydligare de senaste åren eftersom att antalet attacker mot populära sajter som Facebook, YouTube och Google också ökat. Anledningarna till en sådan attack kan vara olika, från en regering som vill kontrollera sina invånare till kriminella organisationer som antingen vill lura åt sig pengar eller sälja uppgifterna till någon som vill använda dem.

Kryptografi är alltså en viktig del av den tekniska vardagen, men sker oftast utan att vi märker av den.

För en vidare diskussion om moderna chiffer se Stinsons bok *Cryptography: Theory and practice* [8], och för en mer översiktlig bild tillsammans med andra aspekter på säkerhet se Andersons bok *Security Engineering* [4].

Referenser

[1] crypto-, comb. form. I: *OED Online*. Oxford University Press, mar 2013. URL `http://www.oed.com/view/Entry/45363`. Hämtad den 5 april 2013.

[2] cryptography, n. I: *OED Online*. Oxford University Press, mar 2013. URL `http://www.oed.com/view/Entry/45374?redirectedFrom=cryptography&`. Hämtad den 5 april 2013.

[3] graphy-, comb. form. I: *OED Online*. Oxford University Press, mar 2013. URL `http://www.oed.com/view/Entry/80855`. Hämtad den 5 april 2013.

[4] Anderson, Ross J. *Security engineering : a guide to building dependable distributed systems*. Wiley, Indianapolis, IN, 2nd ed. utgåvan, 2008. ISBN 978-0-470-06852-6 (hbk.).

[5] Kelly, Thomas. The myth of the skytale. *Cryptologia*, 22(3), 1998.

[6] Shannon, C. E. Communication theory of secrecy systems. *Bell Systems Technical Journal*, 28:656–715, 1949.

[7] Singh, Simon. *The code book : the secret history of codes and codebreaking*. Fourth estate, London, paperback ed. utgåvan, 2000. ISBN 1-85702-889-9.

[8] Stinson, Douglas R. *Cryptography : theory and practice*. Chapman & Hall/CRC, Boca Raton, 3. ed. utgåvan, 2006. ISBN 1-58488-508-4 (Hardcover).

[9] Wikipedia. Scytale, 2011. URL `https://en.wikipedia.org/wiki/File:Skytale.png`. Hämtad den 20 juni 2011.

[10] Wikipedia. Letter frequency, 2012. URL `https://en.wikipedia.org/wiki/Letter_frequency`. Hämtad den 1 oktober 2012.