Universiteit van Stellenbosch

Toegepaste Wiskunde 314

Tutoriaal 3: Donderdag 4 Maart 2004

(1) (a) Enkripteer, *met die hand*, die skoonteks `inthedesertsoftheheart` volgens die permutasie substitusie stelsel $\Pi_{26}^{\pi_1}$, waar π_1 gegee word deur:

a	b	c	d	e	f	g	h	i	j	k	l	m
Z	H	I	F	P	Q	J	M	X	N	R	Y	K

n	o	p	q	r	s	t	u	v	w	x	y	z
L	T	S	U	W	B	D	E	C	V	A	G	O

(b) Toets die korrektheid van jou antwoord deur middel van die program **EnDeCrypt**. [Wenk: Klik op "Crypto systems" op die **EnDeCrypt** hoofspyskaart, daarna op "Block ciphers", en daarna op "Permutation substitution".]

(2) Die kriptoteks `YPDDMPMPZYXLJQTELDZXLBDZWD` is deur middel van die permutasie substitusie stelsel $\Pi_{26}^{\pi_1}$ gevorm.

(a) Dekripteer die kriptoteks *met die hand*.

(b) Toets die korrektheid van jou antwoord aan die hand van die program **EnDeCrypt**.

(3) Die kriptoteks

```
YNCPWUQXVODYQWPCYOOPWOQJWQWWQWPOPPWOAQXOZMAPWAQVVAJXOEPXVPBGYZHYGGPCB
YQCJWIJOAVQCPVMYVBNIGQVAPCQWOVPGQJOVBPXQJCQHYGOAPHXQOPXQJWQWOAPVYSPZP
YXYBBPYXPCYNCPWVBJPSVAQVUQXVOHJSSPXHQYGGZBNIGQVAPCIJJTQWMAQHAAPHYXPUN
GGZYEJQCPCZPYOVQYWXJSYWOQHVPGUPRBXPVVQJWOAPBJPSVMPXPVAJXONWOQOGPCYWCV
GQDAOGZHXZBOQHYNCPWVJJWDYQWPCUYSPYVYGPUOQVOQWOPGGPHONYGAPVAJMPCQWOPXP
VOQWSYXRYWCUXPNCYWCAPMXJOPBYVVQJWYOPGZJWVJHQYGBXJIGPSVYSJWDJOAPXVQWGJ
JTVOXYWDPXQWWQWPOPPWOAQXOZVQRHJSBXPVVPCUQDNXPVJUVBPPHACQXPHOVOYOPSPWO
YWCSNVQHYGPUUPHOHAYXYHOPXQFPCJWOAQVQVGYWCQWWQWPOPPWOAQXOZVPEPWYWCYWJO
APXOQSPQWWQWPOPPWUJXOZQWOAPGYOPWQWPOPPWOAQXOQPVYNCPWVBJPSVMPXPBPXAYBV
GPVVXYCQHYGBJGQOQHYGGZVNUUPXQWDYWCQWLNVOQHPYXPWJOXPLPHOPCYVYBYXOJUJXC
QWYXZGQUPOAPGYVOMJXTVUXJSOAQVCPHYCPYVOJWQVAPCXPYCPXVMQOAOAPQXGQDAOHJS
QHOJWPYWCCJSPVOQHQOZ
```

(bestaande uit 779 karakters) is deur middel van die permutasie substitusie stelsel $\Pi_{26}^{\pi_2}$ gevorm.

(a) Gebruik letterfrekwensie–tegnieke om vas te stel wat die waarskynlike natuurlike taal van die onderliggende skoonteks is.

(b) Gebruik die program **EnDeCrypt** en die letterfrekwensies in die bostaande kriptoteks om die sleutel π_2 te vind en sodoende die onderliggende skoonteks te ontrafel.

(4) Vir 'n sekere kriptoteks van lengte 16 374 karakters (wat met behulp van die permutasie substitusie–stelsel $\Pi_{26}^{\pi_3}$ gevorm is) word die volgende letterfrekwensie tellings verkry:

A:	1165	J:	30	S:	962
B:	250	K:	82	T:	1468
C:	399	L:	727	U:	401
D:	815	M:	380	V:	149
E:	1928	N:	1076	W:	554
F:	398	O:	1396	X:	32
G:	294	P:	294	Y:	287
H:	966	Q:	9	Z:	8
I:	1152	R:	1152		

In watter taal is die ooreenstemmende skoonteks na alle waarskynlikheid?

(5) (a) Enkripteer *algebraïes* en *met die hand*, die skoonteks `whauden` ("WH Auden") volgens die Vigenère stelsel $\vartheta_{26}^{7,\underline{s}_2}$, met kodewoord $\underline{s}_1 =$ `wills`.

(b) Toets die korrektheid van jou antwoord deur dieselfde enkripsie aan die hand van die Vigenère tabel op bladsy 53 van die klasnotas te herhaal.

(c) Toets nogmaals die korrektheid van jou antwoord deur middel van die program **EnDeCrypt**. [Wenk: Klik op "Crypto systems" op die **EnDeCrypt** hoofspyskaart, daarna op "Block ciphers", en daarna op "Vigenère substitution".]

(6) (a) Dekripteer *algebraïes* en *met die hand*, die kriptoteks `EUTDLPNPSKUOBOIOKAUZTA HCDAHAMRALMWUHKDTKWRWPSA` volgens die Vigenère substitusie stelsel $\vartheta_{26}^{8,\underline{s}_2}$, met kodewoord $\underline{s}_2 =$ `WHA`.

(b) Toets die korrektheid van jou antwoord deur dieselfde dekripsie aan die hand van die Vigenère tabel op bladsy 53 van die klasnotas te herhaal.

(c) Toets nogmaals die korrektheid van jou antwoord deur middel van die program **EnDeCrypt**.

(7) Probleem 11(a) op bladsy 81 van die klasnotas. Die kriptoteks wat ter sprake is, word volledigheidshalwe hier weergegee as:

```
ZHYWKYEHLAGLCVWGBYZATDWGFMROWFIEMOSYAFJWGDSMKKDCFLNEMWNKNNWWTTBSFJEC
YZZEYFLNCYFLARCWKGNXESTYMHWIIUDXGCNKUUNWWJTIHYUUNAJMKNWWKCELWFUTYVXU
RYPSSPFWLNEWGFMROWFIEMGXLELESZEODWXAHVOOLMGFJANWXXOGLZOSJWJOOXVMXIHY
LNEYAYNTYWFZHWWFZULQXARNZWXCIFLXIVMLOOHKOKRYESJEVQDGGLSFMEUFVREASFJR
YZGCEPWJZHYJWGLVAJZHIXUUNAJMKNWWKGSUUGNELWFZTBWGXYIUUARLWVON1799QALN
TBWHABFAUGTCGFUFASMYSXAKWUCKAZIIFWYMULZKMULAIAYALCAMYSASMOZUFCJKZSSK
LKMULAIAFDQYTOVAKDWGFMROWFIEMXGXTBWAXOQFKGKYSFJWBGATTLGVACYVLNEWGFBE
HAWTTHGLGTCGFYTCDDONOKW
```

Steers Uitdaging: Ontrafel die betekenis van die kriptoteks

```
PHZOLHONONSHYYUMABKKHLQHSFZOLXUNZILLBLUWLVGYRUTKABKSPPOUNHGA
PITZDUOALUIOZYWBLMZLYYJPUCZZOUZL,
```

wat met behulp van die Vigenère stelsel $\vartheta_{26}^{n,\underline{s}_3}$ gevorm is.