

Tentamen Cryptografie

25 maart 2004

1. [15 punten] – Klassieke systemen

- Ontcijfer de navolgende kolomtranspositie EMZRM PAAAR EDNTW ICKND AXIJA GDUDO BHALA XTSEP OAKPN IDUDU EUTTO E met sleutel VERTAALOEFFENING.
- Waarin verschillen polyalfabeten als de Vigeère en de Beaufort van het multiplex geheimschrift zoals de M94 en de Bazeries cilinder?
- Vercijfer de navolgende tekst MAKKERS STAAKT UW WILD GERAAS met sleutel DONDERSTEEN in het Beaufort systeem; kies daartoe de goede uit de onderstaande twee polyalfabetische tableaux.

???-tabel

	ABCDEFGHIJKLMN	OPQRSTUVWXYZ	
A	ABCDEFGHIJKLMN	OPQRSTUVWXYZ	A
B	BCDEFGHIJKLMN	OPQRSTUVWXYZA	B
C	CDEFGHIJKLMN	OPQRSTUVWXYZAB	C
D	DEFGHIJKLMN	OPQRSTUVWXYZABC	D
E	EFGHIJKLMN	OPQRSTUVWXYZABCD	E
F	FGHIJKLMN	OPQRSTUVWXYZABCDE	F
G	GHIJKLMN	OPQRSTUVWXYZABCDEF	G
H	HJKLMN	OPQRSTUVWXYZABCDEFGH	H
I	IJKLMN	OPQRSTUVWXYZABCDEFGHI	I
J	JKLMN	OPQRSTUVWXYZABCDEFGHIJ	J
K	KLMN	OPQRSTUVWXYZABCDEFGHIJK	K
L	LMN	OPQRSTUVWXYZABCDEFGHIJKL	L
M	MN	OPQRSTUVWXYZABCDEFGHIJKLM	M
N	NO	OPQRSTUVWXYZABCDEFGHIJKLMN	N
O	OP	QRSTUVWXYZABCDEFGHIJKLMNO	O
P	PQ	RSTUVWXYZABCDEFGHIJKLMNO	P
Q	QR	STUVWXYZABCDEFGHIJKLMNO	Q
R	R	STUVWXYZABCDEFGHIJKLMNO	R
S	S	TUVWXYZABCDEFGHIJKLMNO	S
T	T	UVWXYZABCDEFGHIJKLMNO	T
U	U	VWXYZABCDEFGHIJKLMNO	U
V	V	WXYZABCDEFGHIJKLMNO	V
W	W	XYZABCDEFGHIJKLMNO	W
X	X	YZABCDEFGHIJKLMNO	X
Y	Y	ZABCDEFGHIJKLMNO	Y
Z	Z	ABCDEFGHIJKLMNO	Z

???-tabel

	ABCDEFGHIJKLMN	OPQRSTUVWXYZ	
A	AZYXWVUTSRQP	ONMLKJIHGFEDCB	A
B	BAZYXWVUTSRQP	ONMLKJIHGFEDC	B
C	CBAZYXWVUTSRQP	ONMLKJIHGFED	C
D	DCBAZYXWVUTSRQP	ONMLKJIHGFED	D
E	EDCBAZYXWVUTSRQP	ONMLKJIHGFED	E
F	FEDCBAZYXWVUTSRQP	ONMLKJIHGFED	F
G	GFEDCBAZYXWVUTSRQP	ONMLKJIHGFED	G
H	HGFEDCBAZYXWVUTSRQP	ONMLKJIHGFED	H
I	IHGFCBZYXWVUTSRQP	ONMLKJIHGFED	I
J	JIHGFEDCBZYXWVUTSRQP	ONMLKJIHGFED	J
K	KJIHGFEDCBZYXWVUTSRQP	ONMLKJIHGFED	K
L	LKJIHGFEDCBZYXWVUTSRQP	ONMLKJIHGFED	L
M	MLKJIHGFEDCBZYXWVUTSRQP	ONMLKJIHGFED	M
N	NMLKJIHGFEDCBZYXWVUTSRQP	ONMLKJIHGFED	N
O	ONMLKJIHGFEDCBZYXWVUTSRQP	ONMLKJIHGFED	O
P	PONMLKJIHGFEDCBZYXWVUTSRQP	ONMLKJIHGFED	P
Q	QPONMLKJIHGFEDCBZYXWVUTSRQP	ONMLKJIHGFED	Q
R	RQPONMLKJIHGFEDCBZYXWVUTSRQP	ONMLKJIHGFED	R
S	SRQPONMLKJIHGFEDCBZYXWVUTSRQP	ONMLKJIHGFED	S
T	TSRQPONMLKJIHGFEDCBZYXWVUTSRQP	ONMLKJIHGFED	T
U	UTSRQPONMLKJIHGFEDCBZYXWVUTSRQP	ONMLKJIHGFED	U
V	VUTSRQPONMLKJIHGFEDCBZYXWVUTSRQP	ONMLKJIHGFED	V
W	WVUTSRQPONMLKJIHGFEDCBZYXWVUTSRQP	ONMLKJIHGFED	W
X	XWVUTSRQPONMLKJIHGFEDCBZYXWVUTSRQP	ONMLKJIHGFED	X
Y	YXWVUTSRQPONMLKJIHGFEDCBZYXWVUTSRQP	ONMLKJIHGFED	Y
Z	ZYXWVUTSRQPONMLKJIHGFEDCBZYXWVUTSRQP	ONMLKJIHGFED	Z

2. [5 punten] – Statistische methoden

Het tweede moment $\sum_i p_i^2$ van een symbooldistributie speelt in de cryptanalyse een belangrijke rol. Geef een voorbeeld van de toepassing. Geef ook de formule voor het benaderen van dit tweede moment uit een frequentietelling.

3. [15 punten] – Moderne systemen

Beschrijf naar keuze, zo compleet mogelijk, de werking van een der volgende symmetrische geheimschriften: DES, AES of Skipjack.

4. [10 punten] – Moderne systemen

Voor masters:

Leg uit waarop (naar keuze) differentiële dan wel lineaire cryptanalyse berust.

Voor bachelors:

Leg uit hoe de Hellman time-memory trade-off werkt.

Voor beide:

Is de beschreven cryptanalyse ciphertext only, known plaintext of chosen plaintext?

5. [10 punten] – Public Key

Voor masters:

Het ElGamal-systeem verschilt van het RSA-systeem met betrekking tot het herhaald vercijferen van een zelfde bericht; verklaar dit. Beschrijf de werking van dit geheimschrift. Waarop berust de veiligheid bij ElGamal?

Voor bachelors:

Leg uit wat wordt bedoeld met Elliptic Curve Cryptography (ECC). Wat is het nut van ECC in vergelijking met het werken met (priem)getallen?

6. [15 punten] – Informatietheorie

- Gegeven is een symbooldistributie p_A, p_B, \dots, p_Z voor de 26 letters van het alfabet. Geef de formule voor de entropie van deze distributie. Voor welke distributie neemt deze entropie de minimale dan wel de maximale waarde aan? Hoe groot zijn deze extreme waarden?
- Wat wordt verstaan onder een Markov keten en hoe kan de entropie hiervan worden berekend?
- Leg uit wat in de cryptografie met het begrip ‘unicity distance’ wordt bedoeld.

7. [5 punten] – Schuifregisters

We vatten $\frac{1}{f(x)}$ op als schuifregisterrij en stellen $f(x) = g(x) \cdot h(x)$, $g(x) \neq h(x)$. De graad van resp. $f(x)$, $g(x)$ en $h(x)$ stellen we op n_f , n_g en n_h . We ontbinden

$$\frac{1}{f(x)} = \frac{s(x)}{g(x)} + \frac{t(x)}{h(x)}$$

Laat zien dat $f(x)$ geen maximaal-rij oplevert.

8. [15 punten] – Schuifregisters

- Een bepaalde combinatie van drie schuifregisters S_1 , S_2 en S_3 heeft de nevenstaande productietabel. Bepaal de terugkoppel-functie (in algebraïsche normaalvorm).
- Wat beoogt men te bepalen met een ‘correlatie aanval’? Tegen welke van de bovengenoemde drie deelstromen kan met succes een correlatie aanval worden ondernomen en waarom?
- Geef een beknopte beschrijving van het Pless systeem voor gecombineerde lineaire schuifregisterstromen. Waarom kan hierbij niet worden volstaan met een combinatie van slechts schuifregisterstromen?

S_1	S_2	S_3	S
0	0	0	1
0	0	1	1
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	0