

Werk deze opgaven uit op het tentamenpapier

Opgave-1

5

1. Wat wordt bedoeld met een *endomorf* cryptosysteem?
2. Wanneer is dit van belang?
3. Welke van de navolgende systemen zijn endomorf?
Vigenère, monome-dinome, transpositie, cijfercode.

Opgave-2 Maak in twee stappen een gepermuteerd alfabet uit het standaardalfabet.

5

1. Maak als eerste stap een alfabetpermutatie gebaseerd op het sleutelwoord VALSCHERM.
2. Onderwerp in stap twee het resultaat van de vorige operatie aan een enkelvoudige kolomtranspositie met onuitgevulde laatste kolom; gebruik wederom VALSCHERM als sleutel, nu voor de transpositie. Toon het ingevulde transpositieblok met bovenaan de sleutel en geef de uit deze transpositie resulterende finale alfabetsleutel.

Opgave-3

5

FDQIOZ FJB VDWUR FXIJRZANZIAG PI ASCK OWJAGZ
FIOLN VAN TOORN OVERSPOELDEN DE ARME DOCENT

Bovenstaand cijfertekst/plaintext paar is in Beaufort vercijferd. Bepaal de gebruikte periodieke sleutel; twee periodes is voldoende om die met zekerheid te kunnen vaststellen.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A:	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B
B:	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C
C:	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D
D:	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E
E:	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F
F:	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G
G:	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H
H:	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I
I:	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J
J:	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K
K:	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L
L:	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M
M:	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N
N:	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O
O:	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P
P:	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q
Q:	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R
R:	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S
S:	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T
T:	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U
U:	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V
V:	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W
W:	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X
X:	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y
Y:	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z
Z:	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

Opgave-4

10

1. Geef een gedetailleerde beschrijving van de Purple vercijfermachine.
2. Hoe werd de voorloper van Purple door de Amerikanen genoemd?
3. Kan Purple een letter tot zichzelf vercijferen?

Opgave-5

10

1. Wat zijn coïncidenties?
2. De aantallen coïncidenties zijn gerelateerd aan de zogenaamde chi-test. Hoe berekent men die waarde voor twee cryptogrammen?
3. Gebruik deze chi-test om van de gegeven distributies A, B en C van drie cryptogrammen te bepalen welke twee cryptogrammen de meeste overeenkomst vertonen.

	0	1	2	3	4	5	6	7	8	9
A	0	2	3	1	3	4	0	1	1	0
B	3	1	1	2	4	4	1	0	0	1
C	2	2	1	1	1	2	1	2	3	1

Opgave-6 De regel van Bayes toegepast op een systeem met berichten M, cryptogrammen C en sleutels K geeft als de voorwaardelijke kans op een bericht M gegeven een cryptogram C:

5

$$P(M|C) = \frac{P(M)P(C|M)}{P(C)}$$

1. Beschrijf in woorden wat dit betekent.
2. Laat zien onder welke omstandigheden de best mogelijke veiligheid wordt bereikt.
3. Geef ook aan wat dit betekent voor het aantal sleutels in sleutelverzameling K.

Opgave-7 Geef een beschrijving van het Feistel-schema voor een geheimschrift. Hoe werken het vercijferen en ontcijferen in dit schema? Hoe wordt de vercijfersleutel gebruikt? Wat zijn de eigenschappen van deze methode?

5

Opgave-8

5

Beschrijf beknopt TripleDES, schenk aandacht aan de verschillende sleutelvarianten. Beschouw enkelvoudig DES als een gegeven dat niet hoeft te worden uitgelegd.

Opgave-9 Geef antwoord op de volgende vragen over het Diffie en Hellman-systeem voor sleuteluitwisseling.

5

1. Welke getalverzameling en basisgetal worden gebruikt in het systeem?
2. Wat voor geheime parameter kiest deelnemer i?
3. Wat maakt deelnemer i openbaar?
4. Hoe berekent deelnemer j de gemeenschappelijke sleutel met deelnemer i?
5. Waarop berust de veiligheid van het systeem?

Opgave-10 Van de vele mogelijkheden om met lineaire schuifregisters een niet-lineaire combinatie te maken wordt gevraagd de *Bruer-generator* te beschrijven.

5