GEBRUIK VAN **ENDECRYPT**, **MATHEMATICA** EN **MATLAB** WORD TOEGELAAT

Universiteit van Stellenbosch
Toegepaste Wiskunde 314
Semestertoets II
12 Junie 2004
Tyd: 09:00-12:00 Punte: 100

Vul asseblief in / *Please complete*:

Van (blokletters) / *Surname (capitals)*
MEMO
Volle Voorname / *Full First Names*
US–nommer / *US Number*

Vir kantoorgebruik / *For official use*

Vraag *Question*	Punte *Marks*	Nasiener *Marker*
1	/21	J. van Vuuren
2	/19	J. van Vuuren
3	/15	P. Grobler
4	/29	P. Grobler
5	/8	P. Grobler
6	/8	P. Grobler
Totaal	/100	

Eksaminatore / Examiners: J.H. van Vuuren & P.J.P. Grobler

Lees asseblief die volgende reëls en voorskrifte, en teken dan die onderstaande verklaring:

(1) Kommunikasie tussen kandidate word nie in die eksamenlokaal toegelaat nie.

(2) Hulpmiddels (insluitende blankopapier, boeke, geskrifte en elektroniese apparaat) word nie in die eksamenlokaal toegelaat nie, tensy die gebruik van spesifieke items uitdruklik toegelaat of voorgeskryf is.

(3) Geen dele van hierdie vraestel/antwoordstel mag verwyder word nie.

(4) Ekstra tyd word nie toegestaan aan kandidate wat laat kom nie.

(5) Kandidate word nie toegelaat om die eksamenlokaal binne die eerste 45 minute van die eksamensessie te verlaat nie.

(6) Antwoorde mag in potlood ingevul word.

(7) Hierdie vraestel sowel as u antwoordstel moet aan 'n opsiener oorhandig word voordat u die eksamenlokaal verlaat.

Please read the following rules and instructions, and then sign the declaration below:

(1) Communication between candidates is not allowed.

(2) Supporting material (including blank paper, books, notes and electronic equipment) is not allowed in the examination room, unless the use of particular items is expressly allowed or prescribed.

(3) No parts of this question/answer paper may be removed.

(4) Latecomers are not allowed extra time.

(5) Candidates are not allowed to leave the examination room within the first 45 minutes of the examination session.

(6) Answers may be supplied in pencil.

(7) Before leaving the examination room candidates must hand this question paper as well as solutions to an invigilator.

VERKLARING / *DECLARATION*	HANDTEKENING / *SIGNATURE*
Hiermee verklaar ek dat ek die bogenoemde eksamenreëls sal gehoorsaam en dat die inligting op hierdie bladsy verstrek, korrek is. / *I hereby declare that I will abide by the above examination rules and that the particulars supplied on this front cover are correct.*	

(1) (a) Verduidelik die verskil tussen 'n *onreduseerbare* polinoom en 'n *primitiewe* polinoom in die ring $(\mathbb{Z}_2, +, \times)$. / *Explain the difference between an* irreducible *polynomial and a* primitive *polynomial in the ring* $(\mathbb{Z}_2, +, \times)$. [2]

'n Polinoom is onreduseerbaar in $(\mathbb{Z}_2[x], +, \times)$ as dit geen nie-triviale faktore in die ring het nie.
'n Polinoom is primitief as dit onreduseerbaar is en maksimale eksponent ($e = 2^m - 1$, met m die polinoom-graad) het.

(b) Gebruik **Mathematica** om te toets of die volgende polinome primitief is in die ring $(\mathbb{Z}_2, +, \times)$, of nie. Motiveer volledig. / *Use* **Mathematica** *to determine whether the following polynomials are primitive in the ring* $(\mathbb{Z}_2, +, \times)$, *or not. Motivate fully.* [5]

i. $f_1(x) = 1 + x^2 + x^6$,

$= (1 + x + x^3)^2 \Rightarrow$ nie onreduseerbaar nie
$\Rightarrow$ nie primitief nie

ii. $f_2(x) = 1 + x^3 + x^6$,

Wel onreduseerbaar; geen faktore
Nie primitief nie; eksponent $e = 9 < 2^6 - 1 = 63$

iii. $f_3(x) = 1 + x^5 + x^6$.

Wel onreduseerbaar; geen faktore
Wel primitief; eksponent $e = 2^6 - 1 = 63$

(c) Gebruik die feit dat die generator–funksie $G(x) = \sum_{i=0}^{\infty} s_i x^i$ wat ooreenstem met 'n binêre stroom $\underline{s} = s_0, s_1, s_2, \ldots$ geskryf kan word as $G(x) = \Psi(x)/f(x)$, waar $\Psi(x)$ 'n polinoom van graad hoogstens $m-1$ in die ring $(\mathbb{Z}_2, +, \times)$ is, en $f(x) = \sum_{i=0}^{m} p_i x^i \in (\mathbb{Z}_2, +, \times)$ die karakterestieke polinoom is van 'n linêre terugvoer skuifregister $\mathcal{F}^m_{f(x)}$ wat $\underline{s}$ genereer, om te bewys dat indien $f(x)$ onreduseerbaar is met eksponent e in die ring $(\mathbb{Z}_2, +, \times)$ en $\underline{s} \neq 0, 0, 0, \ldots$, die periode van $\underline{s}$ presies e is. / *Use the fact that the generator function $G(x) = \sum_{i=0}^{\infty} s_i x^i$ associated with a binary stream $\underline{s} = s_0, s_1, s_2, \ldots$ may be expressed as $G(x) = \Psi(x)/f(x)$, where $\Psi(x)$ is a polynomial of degree at most $m-1$ in the ring $(\mathbb{Z}_2, +, \times)$, and $f(x) = \sum_{i=0}^{m} p_i x^i \in (\mathbb{Z}_2, +, \times)$ is the characteristic polynomial of a linear feedback shiftregister $\mathcal{F}^m_{f(x)}$ that generates $\underline{s}$, to prove that if $f(x)$ is irreducible with exponent e in the ring $(\mathbb{Z}_2, +, \times)$ and $\underline{s} \neq 0, 0, 0, \ldots$, then the period of $\underline{s}$ is exactly e.* [6]

Aangesien die eksponent van $f(x)$ e is, volg dit dat $f(x) \mid (x^e+1)$. Gestel $\underline{s}$ bring die generatorfunksie $G(x) = \Psi(x)/f(x)$ voort, waar $\Psi(x)$ van graad hoogstens $m-1$. Dan is

$$G(x) = \frac{\Psi(x)}{\frac{x^e+1}{g(x)}} = \frac{\Psi(x)\,g(x)}{x^e+1} = \Psi(x)g(x)(1+x^e+x^{2e}+x^{3e}+\ldots)$$

vir een of ander polinoom van graad hoogstens $m-1$, sodat $\underline{s}$ periodies is met periode 'n deler van e. Gestel die periode van $\underline{s}$ is p, met $p<e$. Dan is

$$G(x) = s(x)(1+x^p+x^{2p}+x^{3p}+\cdots) = \frac{s(x)}{1+x^p}$$

waar $s(x) = \sum_{i=0}^{p-1} s_i x^i$. Maar, omdat $G(x) = \Psi(x)/f(x)$, volg dit dat

$$\frac{s(x)}{1+x^p} = \frac{\Psi(x)}{f(x)}$$

sodat $(1+x^p)\Psi(x) = s(x)f(x)$. Aangesien f egter onreduseerbaar is in $(\mathbb{Z}_2[x], +, \times)$, deel dit geen faktore met $\Psi(x)$ nie.

(daar is nog plek om u antwoord op die volgende bladsy voor te sit …/ *there is additional space overleaf to continue your answer …*)

Omdat die graad van $\Psi(x)$ streng kleiner is as m, volg dit dus dat $f(x) \mid (x^p+1)$, wat in teenspraak lewer met die feit dat die eksponent van f $e > p$ is.

Gevolglik is $p \mid e$ en $p \nmid e$ sodat $p = e$.

(d) Gee 'n interpretasie van die betekenis van die funksie $\Psi(x)$ in vraag (c), in die konteks van die lineêre terugvoer skuifregister $\mathcal{F}^m_{f(x)}$. / *Interpret the meaning of the function $\Psi(x)$ in question (c), in the context of the linear feedback shiftregister $\mathcal{F}^m_{f(x)}$.* [2]

Die nie-nul koëffisiënte van $\Psi(x)$ dui die begintoestand posisies van $F^m_{f(x)}$ aan waar daar nie-nul inskrywings is.

(e) Die binêre stroom $\underline{s} = 1,1,1,0,1,0,1,0,1,0,1,1,0,0,1,0,0,\ldots$ is deur middel van 'n lineêre terugvoer–skuifregister, $\mathcal{F}^4_{f(x)}$, gevorm. Gebruik tegnieke uit *lineêre algebra* om die terugvoer–polinoom $f(x)$ te bepaal. / *The binary stream* $\underline{s} = 1,1,1,0,1,0,1,0,1,1,0,0,1,0,0,\ldots$ *was formed by means of a linear feedback shift register,* $\mathcal{F}^4_{f(x)}$. *Use techniques from linear algebra to determine the feedback polynomial,* $f(x)$. [6]

Uit die rekursievergelyking

$$s_j \equiv \sum_{i=1}^{m} p_i s_{j-i} \pmod 2$$

met $f(x) = 1 + \sum_{i=1}^{m} p_i x^i$ en $m=4$

volg dit dat

$$\begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \underbrace{\begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}}_{S} \begin{bmatrix} p_1 \\ p_2 \\ p_3 \\ p_4 \end{bmatrix}$$

sodat

$$\begin{bmatrix} p_1 \\ p_2 \\ p_3 \\ p_4 \end{bmatrix} = \underbrace{\begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}}_{S^{-1}} \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} \equiv \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \pmod 2$$

sodat $f(x) = 1 + x^2$

wat aanleiding gee tot 'n singuliêre LTSR.

(2) (a) Formuleer, sonder bewys, *Fermat se Klein Stelling.* / *Furmulate, without proof,* fermat's Little Theorem. [2]

Gestel $n, x \in \mathbb{N}$ met n priem en $ggd(x,1)=1$.
Dan is $x^{n-1} \equiv 1 \pmod{n}$

(b) Gebruik *Fermat se Klein Stelling* as uitgangspunt en bewys die RSA–sisteem altyd korrek sal werk, met ander woorde dat die dekripsie van die enkripsie van enige versyferde skoonteks, x, weer x is. / *Use* Fermat's Little Theorem *as a point of departure, and prove that RSA system will always function correctly, in other words that the decryption of the encryption of any enumerated plaintext, x, is again x.* [6]

Let op dat $d_n^d(e_n^e(x)) \equiv d_n^d(x^e)^d \equiv x^{ed} \pmod{n}$
vir enige skoontelsversyfering $x \in \mathbb{Z}_n$.
Gevolglik is $ed = i\,\phi(n)+1$ (uit die definisie van die $\phi(n)$ inverse-paar (e,d)), sodat

$$d_n^d(e_n^e(x)) \equiv x^{i\phi(n)+1} \pmod{n} \qquad (*)$$

Nou is $x^{p-1} \equiv 1 \pmod{p}$ vir enige $x \in \mathbb{Z}_n$ uit (a),
sodat $x^{\phi(n)} \equiv x^{(p-1)(q-1)} \equiv (x^{p-1})^{q-1} \equiv 1^{(q-1)} \equiv 1 \pmod{p}$

en gevolglik is

$$x^{i\phi(n)+1} \equiv (x^{\phi(n)})^i x \pmod{p}$$
$$\equiv 1^i x \equiv x \pmod{p} \qquad (**)$$

en net so is

$$x^{i\phi(n)+1} \equiv x \pmod{q} \qquad (***)$$

Deur (**) en (***) in (*) te stel, volg dat

$$d_n^d(e_n^e(x)) \equiv x \pmod{n}.$$

(c) Gebruik *Pollard se Algoritme*, die *Gewysigde Euklidiese Algoritme* en die *Kwadreer–en–Vermenigvuldig Algoritme* om die betekenis van die boodskap 4 026, wat met behulp van die RSA–sisteem deur Persoon A geënkripteer en digitaal onderteken is, en eintlik vir persoon B bedoel is, te ontsyfer. Wys al u werking duidelik. / *Use* Pollard's Algorithm, *the* Revised Euclidean Algorithm *and the* Square–and–Multiply Algorithm *to unravel the meaning of the message* 4 026, *which was encrypted and digitally signed via the RSA system by Person A, and which is actually meant for Person B.* [11]

Persoon / *Person*	n	e
A	7 081	701
B	7 031	607

Pollard om $n_B = 7031$ te faktoriseer: $(a = 15,\ B = 11)$

q	$\lfloor \log n / \log q \rfloor$	a
2	12	6068
3	8	3538
5	5	1669
7	4	3859
11	3	5074

$ggd(a-1, n) = ggd(5073, 7031)$ is 'n faktor van n.
Euklidiese algoritme om hierdie ggd te bereken:

i	p_i	q_i	r_i	s_i
0	7031	5073	1958	1
1	5073	1958	1157	2
2	1958	1157	801	1
3	1157	801	356	1
4	801	356	89	2
5	356	89	0	4
6	89	0	–	–

Dus is 89 'n faktor van 7031 $\Rightarrow$ $7031 = \underbrace{89}_{p_B} \times \underbrace{79}_{q_B}$.

(daar is nog plek om u antwoord op die volgende bladsy voor te sit .../
there is additional space overleaf to continue your answer ...)

$\phi(n_B) = (p_B - 1)(q_B - 1) = 88 \times 78 = 6864$

Bereken d_B mbv die gewysigde Euklidiese algoritme:

i	p_i	q_i	r_i	s_i	x_i	y_i
0	6864	607	187	11	0	1
1	607	187	46	3	1	−11
2	187	46	3	4	−11	34
3	46	3	1	15	34	−147
4	3	1	0	3	−147	2239
5	1	0	—	—	—	—

Gevolglik is $d_B = 2239$.

Berekening van handtekening:

$$k_{A,x} \equiv 4026^{d_B} \pmod{n_B}$$

Mbv kwadreer-en-vermenigvuldig:

$2239 = (100010111111)_2$

i	b_i	z_i	y_i
11	1	1	1
10	0	4026	2221
9	0	2221	4110
8	0	4110	3638
7	1	3638	2702
6	0	1295	3647
5	1	3647	4988
4	1	1152	5276
3	1	525	1416
2	1	5706	4906
1	1	1477	1919
0	1	5856	2549
−1	—	4045	—

Berekening van skoonteks:

$$x \equiv k_{A,x}^{e_A} \pmod{n_A}$$

M bv kwadreer-en-vermenigvuldig:

$701 = (1010111101)_2$

i	b_i	z_i	y_i
9	1	1	1
8	0	4045	4915
7	1	4915	3934
6	0	2023	6792
5	1	6792	5630
4	1	854	7054
3	1	4081	49
2	1	7018	3969
1	0	1978	3772
0	1	3772	2255
−1	—	1147	—

Gevolglik is die skoonteksversyfering $x = 1147$.

(3) (a) Definieer die Hamming afstand $d(\mathbf{x}, \mathbf{y})$ tussen twee vektore $\mathbf{x}$ en $\mathbf{y}$ van $(F_q)^n$.
Define the Hamming distance $d(\mathbf{x}, \mathbf{y})$ *between two vectors* $\mathbf{x}$ *and* $\mathbf{y}$ *of* $(F_q)^n$. [1]

d(x,y) is die aantal posisies waarin x en y verskil.

(b) Bewys dat $d(\mathbf{x}, \mathbf{y}) \leq d(\mathbf{x}, \mathbf{z}) + d(\mathbf{z}, \mathbf{y})$ vir alle $\mathbf{x}, \mathbf{y}, \mathbf{z} \in (F_q)^n$.
Prove that $d(\mathbf{x}, \mathbf{y}) \leq d(\mathbf{x}, \mathbf{z}) + d(\mathbf{z}, \mathbf{y})$ *for all* $\mathbf{x}, \mathbf{y}, \mathbf{z} \in (F_q)^n$. [3]

Note that d(x,y) is the minimum number of changes of digits required to change x to y. We can also change x to y by first making d(x,z) changes from x to z and then making d(z,y) changes from z to y. Hence $d(x,y) \leq d(x,z) + d(z,y)$.

(c) Bewys dat binêre (n, M, d)-kodes met die volgende parameters nie bestaan nie.
Prove that binary (n, M, d)*-codes with the following parameters do not exist.*

i. $(5, 3, 4)$ — bestaan nie! [3]

Veronderstel tot die teendeel dat C 'n (5,3,4)-kode is en gestel s.v.v.a. dat 00000 'n kodewoord is. Dan moet die ander twee kodewoorde elk minstens vier ene bevat. Maar dit impliseer dat hulle in hoogstens twee posisies kan verskil; in teenspraak met d(C) = 4.

ii. $(8, 30, 3)$ [2]

$$M\left\{\binom{n}{0}+\binom{n}{1}\right\} = 30\left\{\binom{8}{0}+\binom{8}{1}\right\} = 270$$

en $2^n = 2^8 = 256$

Dus Hamming se bogrens word nie bevredig nie; dus 'n (8,30,3)-kode bestaan nie.

(d) i. Wys dat 'n ternêre $(3, M, 2)$–kode $M \leq 9$ moet hê.
Show that a ternary $(3, M, 2)$-code must have $M \leq 9$. [4]

Gestel C is 'n ternêre $(3, M, 2)$-kode. Dan moet die M geordende pare wat verkry word deur die derde koördinaat van elke kodewoord weg te laat almal verskillend wees, want sou twee sulke pare identies wees, dan sou die twee ooreenstemmende kodewoorde slegs in die derde posisie verskil, in teenspraak met $d(C) = 2$. Dus is $M \leq 9$.

ii. Vind 'n ternêre $(3, 9, 2)$–kode . / *Find a ternary $(3, 9, 2)$-code .* [2]

$$C = \{000, 101, 202, 011, 112, 210, 022, 120, 221\}$$

is so 'n kode.

(4) (a) Gestel C is 'n nie-triviale deelruimte van $V(n, q)$. Bewys dat enige voortbringerversameling van C 'n basis van C bevat. / *Suppose C is a non-trivial subspace of $V(n, q)$. Prove that any generating set of C contains a basis of C.* [6]

Sien die notas!

(b) Laat C die ternêre lineêre kode wees met voortbringermatriks / *Let C be the ternary linear code with generator matrix*

$$H = \begin{bmatrix} 1011 \\ 2201 \end{bmatrix}$$

i. Lys die kodewoorde van C. / *List the codewords of C.* [2]

0000   2022
1011   1102
2201   0121
0212   1220
2110

ii. Bepaal die minimum afstand van C.
Determine the minimum distance of C. [1]

minimum gewig van die nie-nul kodewoorde is 3 ;
dus $d(C) = 3$.

iii. Is C 'n perfekte kode? (Gee redes). / *Is C a perfect code? (give reasons).* [2]

$9\left\{\binom{4}{0}+\binom{4}{1}(3-1)\right\} = 9\{1+8\} = 81$

en $3^4 = 81$.

Hamming se grens word bevredig ; dus is C 'n perfekte kode .

(c) Laat C die binêre lineêre kode wees met voortbringermatriks
Let C be the binary linear code with generator matrix

$$G = \begin{bmatrix} 10011 \\ 01101 \end{bmatrix}$$

i. Met behulp van neweklasse, stel 'n dekoderingstabel vir C op.
With the aid of cosets, draw up a decoding table for C. [6]

kodewoorde

00000	10011	01101	11110
10000	00011	11101	01110
01000	11011	00101	10110
00100	10111	01001	11010
00010	10001	01111	11100
00001	10010	01100	11111

neweklasleiers

ii. Vind die standaardvorm pariteitskontrolematriks H van C.
Find the standard form parity-check matrix H of C. [2]

$$H = \left[\begin{array}{cc:ccc} 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{array}\right]$$

iii. Skryf die pariteitskontrolevergelykings van C neer.
Write down the parity-check equations of C. [3]

$x_2 + x_3 = 0$

$x_1 + x_4 = 0$

$x_1 + x_2 + x_5 = 0$

iv. Stel die sindroom opsoektabel van C op.
Draw up the syndrome look-up table of C. [3]

neweklas-leier		sindroom
00000	⟶	000
10000	⟶	011
01000	⟶	101
00 00	⟶	100
00010	⟶	010
00001	⟶	001

v. Dekodeer die vektore 11111 en 10101. *Decode the vectors 11111 and 10101.* [4]

$S(11111) = 001$

$\therefore$ fout is 00001

$\therefore$ kodewoord is 11110

$S(10101) = 111$ — nie in opsoektabel nie; dus meer as een fout.

(5) (a) Skryf die pariteitkontrolematriks H vir $Ham(3,2)$ in leksikografiese orde neer.
Write down the parity-check matrix H for $Ham(3,2)$ in lexicographic order. [2]

$$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

(b) Gebruik $Ham(3,2)$ om die ontvangde vektor 1011101 te korrigeer. *Use $Ham(3,2)$ to decode the recieved vector 1011101* . [2]

$S(1011101) = 100$.

Dus fout in posisie $100_2 = 4$;

dus kodewoord is 1010101 .

(c) Gebruik die matriks H in (a) om die pariteitkontrolematriks $\hat{H}$ vir die uitgebreide hammingkode $H\hat{a}m(3,2)$ neer te skryf.
Use the matrix H in (a) to write down the parity-check matrix $\hat{H}$ for the extended hamming code $H\hat{a}m(3,2)$. [2]

$$\hat{H} = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

(d) Gebruik $\hat{H}$ om die vektor 10111001 te korrigeer.
Use $\hat{H}$ to decode the vector 10111001 . [2]

$S(10111001) = 0111$.

Dus fout in posisie $011_2 = 3$;

dus kodewoord is 10011001 .

(6) Laat C die lineêre [10,8]–kode oor $GF(11)$ wees met pariteitskontrolematriks
Let C be the linear [10,8]–code over $GF(11)$ with parity-check matrix

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \end{bmatrix}.$$

(a) Skryf die sindroom $S(\mathbf{y})$ neer van die vektor $\mathbf{y} = y_1y_2 \dots y_{10}$.
Write down the syndrome $S(\mathbf{y})$ of the vector $\mathbf{y} = y_1y_2 \dots y_{10}$. [2]

$$S(y) = \left(\sum_{i=1}^{10} y_i \, , \, \sum_{i=1}^{10} i y_i \right)$$

(b) Neem aan dat 'n enkelfout van grootte k in posisie j van 'n kodewoord $\mathbf{x}$ gemaak was. Vind die sindroom van die resulterende vektor $\mathbf{y}$.
Assume that a single error of magnitude k was made in position j of a codeword $\mathbf{x}$. Find the syndrome of the resultant vector $\mathbf{y}$. [2]

$$S(y) = \left(\left(\sum_{i=1}^{10} x_i \right) + k \, , \, \left(\sum_{i=1}^{10} i x_i \right) + jk \right)$$

$$= (k, jk) \quad \text{aangesien} \quad S(x) = (0,0).$$

(c) Gebruik C om die ontvangde vektore 0617960587 en 3617960587 te dekodeer.
Use C to decode the received vectors 0617960587 and 3617960587.

[4]

S(0617960587) = (5, 9) ;

dus k = 5 en j = 4 en

dus is die kodewoord

0617960587 − 0005000000

= 0612960587 .

S(3617960587) = (8, 1) ;

dus k = 8 en j = 7 en

dus is die kodewoord

3617960587 − 0000008000

= 3617963587 .