cezaris meTodi.

anbanis yovel simbolos Seesabameba garkveuli ricxvi, mag. anbanis rigiTi

nomeri, misi adgilmdebareobis mixedviT. teqstis yovel simbolos (informacia)

emateba fiqsirebuli simbolo (gasaRebi, sigrZe aris erTis toli), ikribeba maTi

Sesabamisi ricxvebi fiqsirebuli moduliT, romelic tolia anbanSi simboloebis

raodenobisa da iwereba miRebuli ricxvis Sesabamisi simbolo. magaliTad:

informacia: A B C D E

gasaRebi: D D D D D

kriptograma: E F G H I

viJineris meTodi

analogiuria, mxolod im gansxvavebiT, rom informacia dayofilia

blokebad. Sifri warmoadgens ara erT simbolos, aramed mTel bloks. blokis

SigniT daSifvra xdeba analogiurad: yovel simbolos emateba Sifris Sesabamisi

simbolo (gadayvanili ricxvebSi). magaliTad:

informacia: N O W I S T H E

blokuri gasaRebi: G A H G A H G A

kriptograma: T O D O S A N E

vernamis meTodi.

mTeli L sigrZis teqsti iSifreba misi sigrZis toli K SifriT L=K.

daSifvra da deSifracia xdeba analogiurad. es aris gauxsneli meTodi, Tu erTi

Sifri gamoiyeneba mxolod erTxel, ix. grafiki 1. [6,7].

Sebrunebuli matricis meTodi.

es meTodi mdgomareobs SemdgomSi:

A matricas irCevs erT-erTi mxare, ugzavnis meore mxares daxuruli arxiT.

A matrica gamoiyeneba informaciis dasaSifrad, xolo misi Sebrunebuli matrica

ki, informaciis gasaSifrad. A matricas moeTxoveba, rom iyos gadaugvarebeli (e.i.

determinanti 0-is toli ar unda iyos), raTa gaaCndes Sebrunebuli.

informacia iyofa garkveuli sigrZis blokebad, blokSi Semavali elementebis raodenoba, damokidebulia matricis ganzomilebaze.

Sifracia mimdinareobs Semdegnairad:

X momxmarebeli sawyis informacias x-s gaamravlebs AA matricaze da miiRebs

daSifrul teqsts.

Y – momxmarebeli miRebuls amravlebs A¯¹ – miiRebs sawyis x–informacias.

x · A = b  b · A¯¹ = x, radgan A · A¯¹ = E