კრიპტოგრაფიის სიმეტრიული სისტემის მეთოდების რეალიზაციის შესახებ MS Exsel-ის გარემოში

გულბაათ ნარიშელაშვილი, ვალერიან კეკელია, იბრაიმ დიდმანიძე
საქართველოს ტექნიკური უნივერსიტეტი

რეზიუმე

შემოთავაზებულია კრიპტოგრაფიის სიმეტრიული სისტემის მეთოდების (ცეზარის, ვიჟინერის, ვერნამის და შებრუნებული მატრიცის) ბაზაზე დამუშავებული ტექსტური ინფორმაციის დაშიფვრა/გაშიფვრის მარეალიზებელი ალგორითმები და მათი პრაქტიკული რეალიზაციის ზოგადი პრინციპები გამოყენებითი პროგრამული უზრუნველყოფის პაკეტის MsOffice-ის ერთ-ერთი კომპონენტის MsExcel-ის ინსტრუმენტულ პროგრამულ გარემოში, რაც აძლევს პიროვნებებს საშუალებას გამარტივებული სახით წარმოადგინონ დაშიფვრა/გაშიფვრის მარეალიზებელი პროცედურები, გაცვალონ ერთმანეთში ინფორმაცია (მოკლეტექსტური შეტყობინებები) ანუ ისაუბრონ „კრიპტოგრაფიის ენაზე".

საკვანძო სიტყვები: კრიპტოგრაფია. საწყისი ტექსტური ინფორმაცია. შიფროტექსტი. საიდუმლო გასაღები. პროგრამული მოდული.

1. შესავალი

მოცემულ ნაშრომში განხილულია სიმეტრიული სისტემის დაშიფვრა/გაშიფვრის მეთოდები, რომლებიც პირობითად გაყოფილია ორ დამოუკიდებელ ქვესისტემად. პირველს მიეკუთვნება ე. წ. უნივერსალური მოდელი, ხოლო მეორეს შებრუნებული მატრიცის მეთოდი [1]. ცნობილია, რომ ეს მეთოდები ძირითადად დაფუძნებულია ერთიდაიმავე პრინციპზე, რომლის ძირითადი არსი მდგომარეობს დასაშიფრ (გასაშიფრ) ტექსტურ ინფორმაციაში - TI შემავალ სიმბოლოებზე წინასწარ განსაზღვრული მათემატიკური და ლოგიკური მანიპულაციების განხორციელებაში.

განიხილავენ TI წარმოდგენის სამ სახეს [1]:

ა) დასაშიფრი TI ანუ საწყისი TI – STI ;

ბ) დაშიფრული TI – ShifTI (შიფროტექსტი);

გ) TI -ის დამშიფრავი (გამშიფრავი) დახურული (საიდუმლო) გასაღები - DamTI.

შევნიშნოთ, რომ სამივე სახის TI წარმოადგენს პერსონალური კომპიუტერის კლავიატურიდან შეტანილი სიმბოლოების ნაკრებისაგან ფორმირებულ სტრიქონს, კერძოდ: $STI = \{S_1 S_2 \ldots S_m\}$, $ShifTI = \{D_1 D_2 \ldots D_m\}$, $DamTI = (K_1 K_2 \ldots K_m\}$,

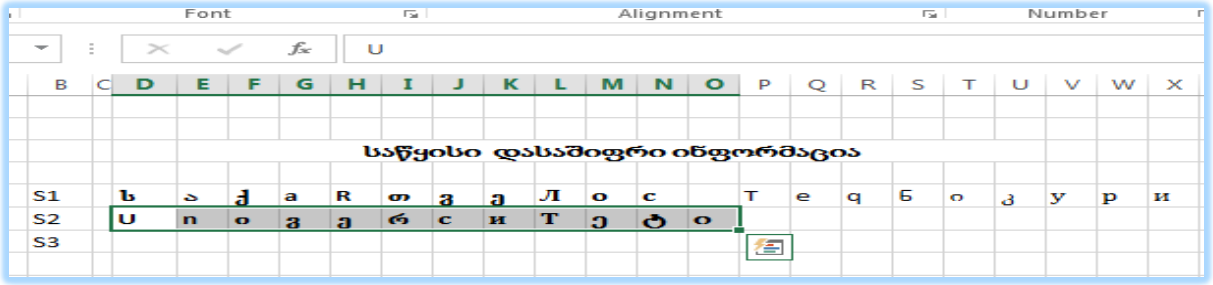
სადაც m და n - აღნიშნავს აღწერილ სტრიქონში შემავალი სიმბოლოების რაოდენობას ანუ მოცემული სტრიქონის სიგრძეს ($n <= m$).

2. ძირითადი ნაწილი

ნაშრომებში [1-4] აღწერილია სიმეტრიული სისტემის მეთოდების მარეალიზებელი ალგორითმის პროგრამული მოდულები (პროგრამა - დანართები (Application)), შემუშავებული ობიექტ-ორიენტირებბულ ენაზე - C#, დაპროგრამირების ენაზე C++ და ა. შ., ფუნქციონირებადი Microsoft Visual Studio .NET გარემოში.

მოცემულ ნაშრომში შემოთავაზებულია როგორც უნივერსალური მოდელის (დამუშავებული ცეზარის, ვიჟინერის და ვერნამის მეთოდების ბაზაზე [1]), ასევე შებრუნებული მატრიცის მეთოდით TI დაშიფვრა/გაშიფვრის ალგორითმების რეალიზაცია MS Excel-ის ინსტრუმენტალურ-პროგრამულ გარემოში, რაც არ მოითხოვს დაპროგრამების ენებისა და მათი ფუნქციონირების უზრუნველყოფას ისეთ რთულ გარემოში, როგორიცაა, მაგალითად, Microsoft Visual Studio .NET გარემო. იგულისხმება, რომ დაშიფვრის და გაშიფვრის ალგორითმებში, გამოყენებულია ქართული –LitNusx, AcadNusx და სხვ., ინგლისური–EN (ლათინუირი ალფაბეტი), რუსული - RU ენების ფონტების შემცველი სიმბოლოების ნაკრებები და მათი შესაბამისი რიცხვითი კოდების მნიშვნელობები, რომლებიც ფიქსირდება კომპიუტერში MS Excel-ის ჩატვირთვის შედეგად. შევნიშნოთ, რომ MS Excel-ში გამოყენებული სიმბოლოების ჯამური ნაკრების რაოდენობა არ აღემატება 256, აქედან ცხადია რომ S_{max} სიმბოლოს მაქსიმალური რიცხვითი კოდური მნიშვნელობა ტოლია 255.

განვიხილოთ STI დაშიფვრის კონკრეტული მაგალითი (ნახ.1).



ნახ. 1

S1 სტრიქონში შეტანილია დასაშიფრი STI, რომელიც ფორმირებულია ინგლისურ, რუსულ და ქართულ ფონტებში შემავალი სიმბოლოებით. S2 სტრიქონში შეტანილია მოცემული STI-ის დამშიფრავი (გამშიფრავი) დახურული (საიდუმლო) გასაღები –DamTI. შევნიშნოთ, რომ რადგან გასაღებში შემავალი სიმბოლოების რაოდენობა მეტია ერთზე და ნაკლებია სტრიქონში შემავალი სიმბოლოების რაოდენობაზე (1<n<m) STI დაშიფვრა-/გაშიფვრა შესრულდება უნივერსალური მოდელის ვიჟინერის მეთოდით [1]. არჩეული (უნივერსალური მოდელის) მეთოდის რეალიზაციის ალგორითმები აღიწერება შემდეგი მათემატიკური ფორმულის სახით:

$$D_i^k=(S_i^k+K_i^k) \bmod 256 \quad \text{(დაშიფვრა)}; \; S_i^k=(D_i^k-K_i^k+256) \bmod 256 \quad \text{(გაშიფვრა)},$$

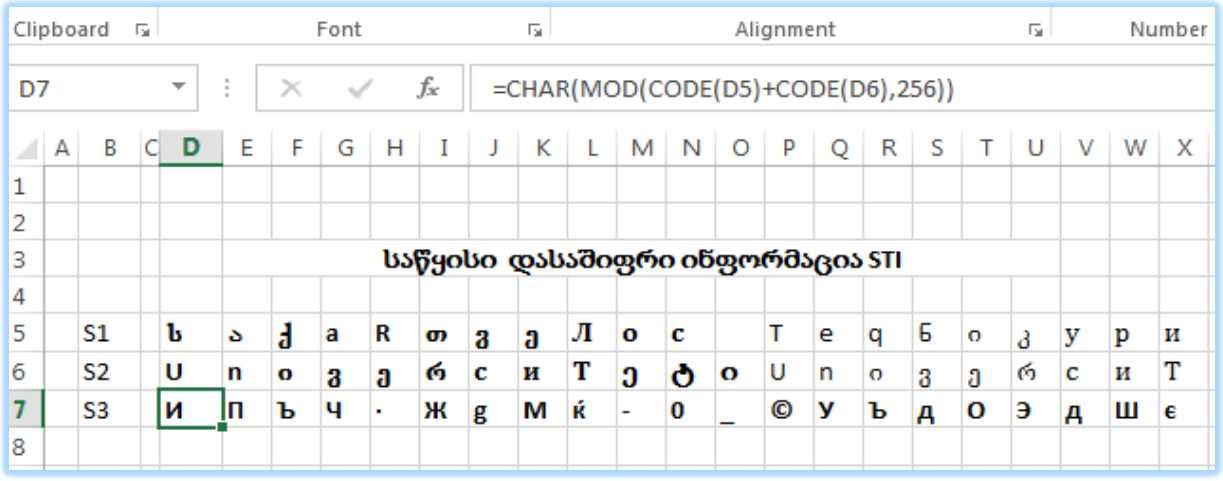
სადაც S_i^k ,D_i^k და K_i^k დასაშიფრი, შიფროტექსტის და საიდუმლო გასაღების S1, S2, S3 სტრიქონების i-ურ პოზიციაში განთავსებული სიმბოლოების რიცხვითი კოდების მნიშვნელობებია.

STI დაშიფვრის პროცედურა შედგება შემდეგი ეტაპებისგან:

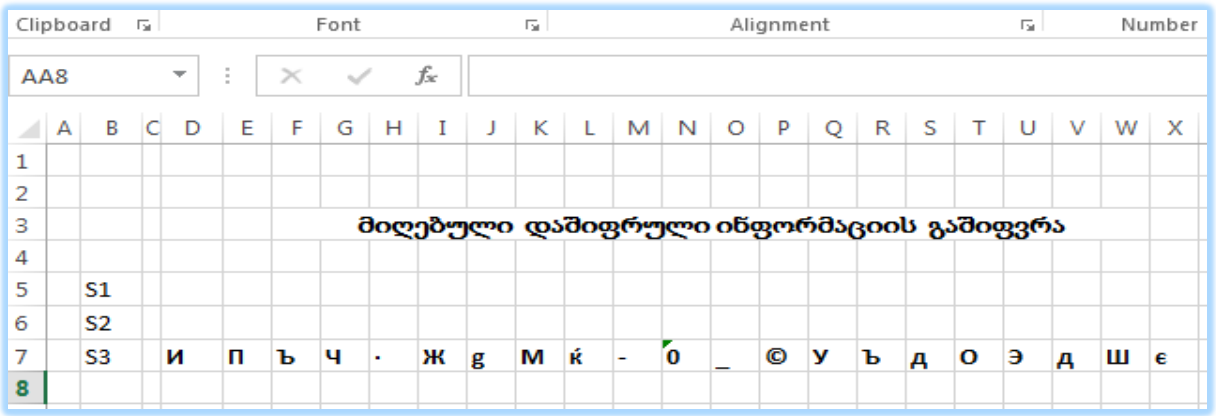
ა) მოვნიშნოთ გასაღები სიტყვა და გადავათრიოთ იგი დასაშიფრი ტექსტის ბოლო სიმბოლომდე (ნახ. 1,2-5);

ბ) მოვნიშნოთ S3 სტრიქონში (უჯრა D7) და შევიტანოთ მასში ფორმულა ნაჩვენები ფორმულების ზოლში;

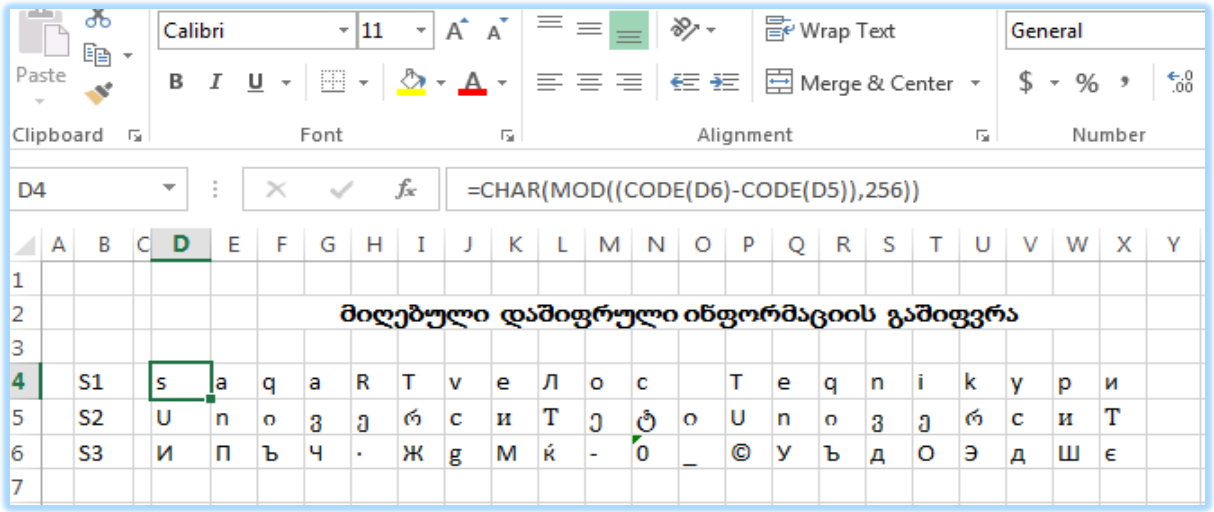
გ) მოვნიშნოთ მიღებული სიმბოლო (უჯრაში D7) და გადავათრიოთ იგი დასაშიფრი STI ბოლო სიმბოლომდე.



ნახ.2



ნახ.3



ნახ.4

S3 სტრიქონში მიღებული (უჯრები D7-X7) სიმბოლოების ერთობლიობა შეადგენს დასაშიფრი STI შიფროტექსტს – ShifTI, რომელიც უნდა გადაეგზავნოს გამშიფრავს. STI დამშიფრავი აფორმირებს ახალ წიგნს - BookNew, რომელშიც გადაწერს ShifTI, შემდეგი ბრძანებების შესრულებით: აკოპირებს მე-7 სტრიქონს – S3 (ნახ.2) და გადაწერს მას ახალი წიგნის ვთქვათ, მე-7 სტრიქონში (ნახ.3) შემდეგი წესით: Past-Paste Special (ფანჯარაში

ავირჩიოთ) Values-OK. დამშიფრავი BookNew-ს გაუგზავნის გამშიფრავს. გამშიფრავი, რომლისათვის ცნობილია საიდუმლო გასაღები, შეიტანს მას S2 სტრიქონში, აფორმირებს DamTI , მონიშნავს D4 უჯრას და შეიტანს მასში ფორმულას, რომელიც ნაჩვენებია ფორმულების ზოლში. შედეგად მიიღება STI-ის პირველი სიმბოლო, რომლის გადათრევით მარჯვნივ ShifTI-ის ბოლო სიმბოლომდე, S1 სტრიქონში დაფიქსირდება STI (ნახ.4).

შევნიშნოთ, რომ დასაშიფრ STI ინფორმაციაში ქართული ფონტის სიმბოლოების გამოსაყენებლად აუცილებელია ამოცანების ზოლში ავირჩიოთ ფონტი დასახელებით EN, ხოლო ინსტრუმენტების პანელიზე ფონტების უჯრაში ქართული ფონტი დასახელებით ვთქვათ, LitNusx, AcadNusx და ა.შ. გარდა აღნიშნულისა დასაშიფრი STI ინფორმაციის კომპაქტური წარმოდგენის მიზნით უნდა მოინიშნოს S1,S2 და S3 სტრიქონის უჯრედები და შესრულდეს შემდეგი ბრძანებები, კერძოდ, Home-Format-Column-Width. ამოტივტივებულ ფანჯარაში საწყისი მნიშვნელობა Column Width = 8,43 უნდა შეიცვალოს, ვთქვათ 3-ით, როგორც ეს შესრულებულია ნახ. 1-4. შევნიშნოთ აგრეთვე, რომ როგორც ნახ. 2 და ნახ. 4 არის ნაჩვენები STI გაშიფვრის შემთხვევაში ქართული სიმბოლოები „საქ“ და „ნიკ“ ჩანაცვლებულია ლათინური სიმბოლოებით, რაც დაკავშირებულია MS Excel-ში ქართული სიმბოლოების არათანმიმდევრული განლაგებით.

განვიხილოთ სიმეტრიული სისტემის მეორე ქვესისტემა (შებრუნებული მატრიცის მეთოდი). ამ მეთოდით ტექსტური ინფორმაციის დასაშიფრავად (გასაშიფრავად) გამოიყენება ორი q – განზომილებიანი DM _ დამშიფრავი და GM – გამშიფრავი ანუ DM-ის შებრუნებული კვადრატული მატრიცა, რომელთა

$$DM=\begin{bmatrix} a_{0,0} & a_{0,1} & a_{0,2} & \dots & a_{0,q} \\ a_{1,0} & a_{1,1} & a_{1,2} & \dots & a_{1,q} \\ \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \\ a_{q,0} & a_{q,1} & a_{q,2} & \dots & a_{q,q} \end{bmatrix} \quad GM=\begin{bmatrix} b_{0,0} & b_{0,1} & b_{0,2} & \dots & b_{0,q} \\ b_{1,0} & b_{1,1} & b_{1,2} & \dots & b_{1,q} \\ \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \\ b_{q,0} & b_{q,1} & b_{q,2} & \dots & b_{q,q} \end{bmatrix}$$

ყოველი წევრი განსაზღვრულია მთელ რიცხვთა სიმრავლეზე. ერთადერთი მოთხოვნა, რაც უნდა იყოს გათვალისწინებული DM მატრიცის შერჩევისას არის ის, რომ მისი დეტერმინანტი (Det) არ უნდა იყოს ნულის ტოლი. თუ გამოთვლების შედეგად აღმოჩნდება, რომ Det=0, მაშინ DM მატრიცაში უნდა შეიცვალოს ზოგიერთი ელემენტის (ერთის მაინც) მნიშვნელობა და ეს ცვლილება უნდა განხორციელდეს მანამ, სანამ არ დაკმაყოფილდება პირობა Det#0. ცნობილია, რომ თუ DM მატრიცის დეტერმინანტი Det#0, მაშინ არსებობს მისი შესაბამისი შებრუნებული მატრიცა GM. ცნობილია აგრეთვე ისიც , რომ თუ DM მატრიცის Det#0 და არსებობს მატრიცა GM , მაშინ არსებობს მატრიცა E, რომელსაც ერთეულოვან მატრიცას უწოდებენ. შევნიშნოთ, რომ E მატრიცაში მთავარ დიაგონალზე განლაგებული ელემენტების მნიშვნელობები ერთის ტოლია.

$$E=DM*GM=\begin{bmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \end{bmatrix}$$

ნაშრომში არ არის მოტანილი დეტერმინანტის, შებრუნებული და ერთეულოვანი მატრიცების გამოთვლების ზოგადი ფორმულები, ვინაიდან მათი მნიშვნელობები განისაზღვრება საოფისე პროგრამის MS Excel-ის სტანდარტული ფუნქციების გამოყენებით, კერძოდ:

ა) დეტერმინანტი გამოითვლება ფუნქციით: MDEთEღM();

ბ) შებრუნებული მატრიცა გამოითვლება ფუნქციით: MMINVEშE();

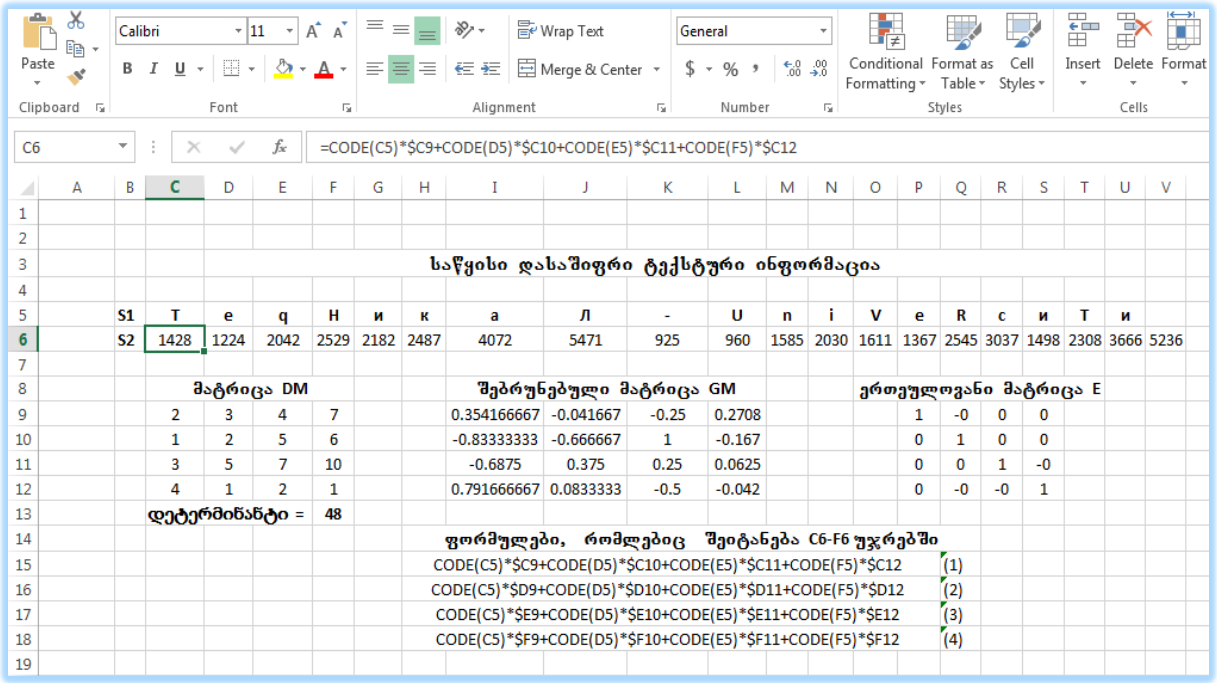
გ) ერთეულოვანი მატრიცა გამოითვლება ფუნქციით: MMULთ().

განვიხილოთ კოკრეტული მაგალითი. მე-5 და მე-7 ნახაზებზე ნაჩვენებია STI ინფორმაციის დაშიფვრისა და გაშიფვრის პროცედურების რეალიზაციის კონკრეტული მაგალითი. დამშიფრავი:

ა) S1 სტრიქონში შეიტანს დასაშიფრ STI {ნახ.5);

ბ) შეადგენს (თავის შეხედულების მიხედვით) დამშიფრავ DM მატრიცას,

გ) გამოთვლის დეტერმინანტს (Det=48).



Paste Clipboard | Calibri 11 | Wrap Text | Merge & Center | General | Conditional Formatting | Format as Table | Cell Styles | Insert | Delete | Format | Font | Alignment | Number | Styles | Cells

C6 =CODE(C5)*$C9+CODE(D5)*$C10+CODE(E5)*$C11+CODE(F5)*$C12

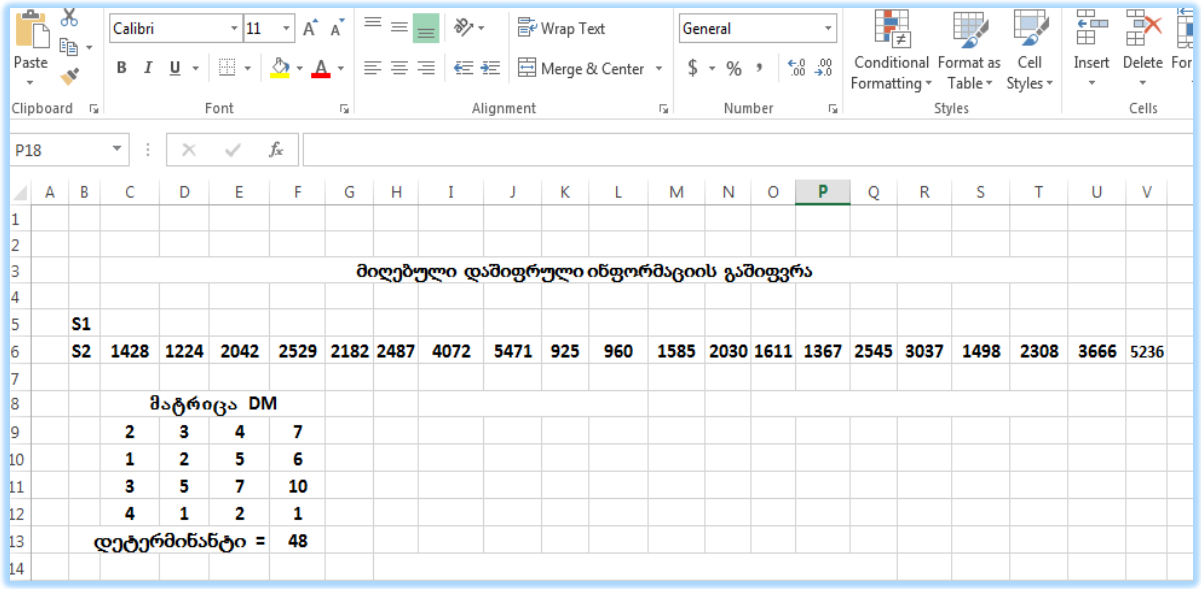
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
1																						
2																						
3									საწყისი დასაშიფრი ტექსტური ინფორმაცია													
4																						
5		S1	T	e	q	H	и	к	a	Л	-	U	n	i	V	e	R	c	и	T	и	
6		S2	1428	1224	2042	2529	2182	2487	4072	5471	925	960	1585	2030	1611	1367	2545	3037	1498	2308	3666	5236
7																						
8			მატრიცა DM						შებრუნებული მატრიცა GM							ერთეულოვანი მატრიცა E						
9			2	3	4	7			0.354166667	-0.041667	-0.25	0.2708				1	-0	0	0			
10			1	2	5	6			-0.83333333	-0.666667	1	-0.167				0	1	0	0			
11			3	5	7	10			-0.6875	0.375	0.25	0.0625				0	0	1	-0			
12			4	1	2	1			0.791666667	0.0833333	-0.5	-0.042				0	-0	-0	1			
13			დეტერმინანტი =			48																
14									ფორმულები, რომლებიც შეიტანება C6-F6 უჯრებში													
15									CODE(C5)*$C9+CODE(D5)*$C10+CODE(E5)*$C11+CODE(F5)*$C12 (1)													
16									CODE(C5)*$D9+CODE(D5)*$D10+CODE(E5)*$D11+CODE(F5)*$D12 (2)													
17									CODE(C5)*$E9+CODE(D5)*$E10+CODE(E5)*$E11+CODE(F5)*$E12 (3)													
18									CODE(C5)*$F9+CODE(D5)*$F10+CODE(E5)*$F11+CODE(F5)*$F12 (4)													
19																						

ნახ. 5

შევნიშნოთ, რომ მე-5 ნახაზზე ნაჩვენებია (შემოწმების მიზნით) შებრუნებული და ერთეულოვანი მატრიცები, თუმცა, უნდა აღინიშნოს, რომ ისინი დამშიფრავს STI-ს დასაშიფრავად არ ჭირდება. შიფროტექსტის მისაღებად, დამშიფრავმა STI უნდა დაყოს ბლოკებად (მარცხნიდან მარჯვნივ): $Б_1, Б_2, ...Б_{t-1}, Б_t$. ყოველ ბლოკში გაერთიანებულია ოთხი სიმბოლო. აღნიშნული რაოდენობა განისაზღვრება DM მატრიცის ზომებით, კერძოდ q-პარამეტრით. მოცემულ შემთხვევაში q=4. ასე მაგალითად, $Б_1$=(T,e,q,H), ..., $Б_t$=(и, T, и). $Б_t$ ბლოკი შედგება სამი სიმბოლოსაგან, ამიტომ იგი უნდა შეივსოს ოთხ სიმბოლომდე.

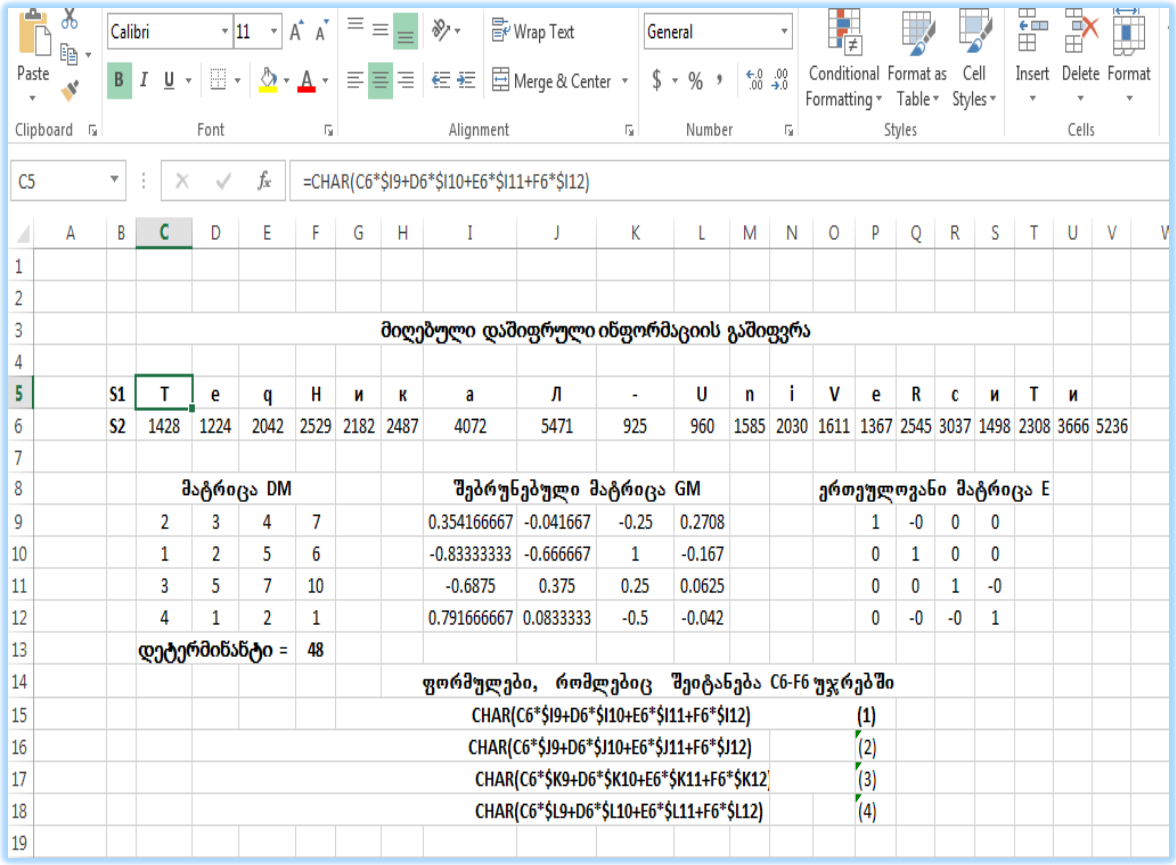
ამ ნახაზზე ნაჩვენებ მაგალითში დასაშიფრ STI ბოლოში დამატებული აქვს სიმბოლო «пробель». შემდეგ დამშიფრავი ახორციელებს $Б_1$–ბლოკის დამუშავებას. კერძოდ, თანმიმდევრობით გამოყოფს S2 სტრიქონში C6, D6, E6, F6 უჯრებს და შესაბამისად შეიტანს

მათში ფორმულებს (1-4) ნაჩვენებს ნახ. 5 (კერძოდ, C6 უჯრაში შესატანი ფორმულა ნაჩვენებია ფორმულების ზოლშიც). მონიშნავს C6, D6, E6, F6 უჯრებს და გადაათრევს მათ დასაშიფრი STI ბოლო სიმბოლომდე. მიღებული რიცხვთა მიმდევრობა არის შიფროტექსტი - ShifTI ={D_1^k D_2^k D_3^k ... D_m^k }, წარმოდგენილი MS Excel-ის ფონტის აბსტრაქტული სიმბოლოების რიცხვითი კოდების მნიშვნელობებით.



3								მიღებული დაშიფრული ინფორმაციის გაშიფვრა													
5		S1																			
6		S2	1428	1224	2042	2529	2182	2487	4072	5471	925	960	1585	2030	1611	1367	2545	3037	1498	2308	3666	5236
8			მატრიცა DM																		
9			2	3	4	7															
10			1	2	5	6															
11			3	5	7	10															
12			4	1	2	1															
13			დეტერმინანტი =			48															

ნახ.6



3									მიღებული დაშიფრული ინფორმაციის გაშიფვრა												
5		S1	T	e	q	H	и	к	a	Л	-	U	n	i	V	e	R	c	и	T	и
6		S2	1428	1224	2042	2529	2182	2487	4072	5471	925	960	1585	2030	1611	1367	2545	3037	1498	2308	3666	5236
8			მატრიცა DM						შებრუნებული მატრიცა GM						ერთეულოვანი მატრიცა E						
9			2	3	4	7			0.354166667	-0.041667	-0.25	0.2708				1	-0	0	0		
10			1	2	5	6			-0.83333333	-0.666667	1	-0.167				0	1	0	0		
11			3	5	7	10			-0.6875	0.375	0.25	0.0625				0	0	1	-0		
12			4	1	2	1			0.791666667	0.0833333	-0.5	-0.042				0	-0	-0	1		
13			დეტერმინანტი =			48															
14									ფორმულები, რომლებიც შეიტანება C6-F6 უჯრებში												
15									CHAR(C6*$I9+D6*$I10+E6*$I11+F6*$I12)							(1)					
16									CHAR(C6*$J9+D6*$J10+E6*$J11+F6*$J12)							(2)					
17									CHAR(C6*$K9+D6*$K10+E6*$K11+F6*$K12							(3)					
18									CHAR(C6*$L9+D6*$L10+E6*$L11+F6*$L12)							(4)					

ნახ.7

STI დამშიფრავი აფორმირებს ახალ წიგნს - BookNew, რომელშიც გადაწერს მატრიცა DM და ShifTI კოდურ მნიშვნელობებს (ნახ.6), შემდეგი ბრძანებების შესრულებით: აკოპირებს მე-6 სტრიქონის – S2 (ნახ.5) და ჩაწერს მას ახალი წიგნის ვთქვათ, მე-6 სტრიქონში (ნახ.6) შემდეგი წესით: Past - Paste special- (გამოსულ ფანჯარაში ავირჩიოთ) - values – OK. დამშიფრავი BookNew გაუგზავნის გამშიფრავს. გამშიფრავი მიიღებს რა დამშიფრავისაგან გამოგზავნილ ინფორმაციას, გამოთვლის დეტერმინანთს, შებრუნებულ და ერთეულოვან მატრიცებს. გამშიფრავმაც STI მისაღებად, უნდა დაყოს იგი ბლოკებად (მარცხნიდან მარჯვნივ): $Б_1, Б_2, ...Б_{t-1}, Б_t$. შემდეგ გამშიფრავი ანხორციელებს $Б_1$–ბლოკის დამუშავებას. კერძოდ, მიმდევრობით გამოყოფს S1 სტრიქონში C5, D5, E5, F5 უჯრებს და შესაბამისად შეიტანს მათში ფორმულებს (1-4), რომლებიც ნაჩვენებია მე-7 ნახაზზე (კერძოდ, C5 უჯრაში შესატანი ფორმულა ნაჩვენებია ფორმულების ზოლში). მონიშნავს C5, D5, E5, F5 უჯრებს და გადაიტანს მათ შიფროტექსტის ბოლო სიმბოლომდე. შესრულებული მანიპულაციების შედეგი იქნება STI (ნახ.7 სტრიქონი S1).

ლიტერატურა:

1. კეკელია ვ., კოტრიკაძე გ. (2016). კრიპტოგრაფიის სიმეტრიული სისტემის მეთოდები და მოდელები. ნაწ.1, სტუ, თბილისი.

2. კეკელია ვ., (2016), კრიპტოგრაფიის სიმეტრიული სისტემის უნივერსალური მოდელის შესახებ, სტუ, თბილისი.

3 . http://zetblog.ru/programming/200812/криптография-шифр-вернама/

4. http://zetblog.ru/programming/200812/криптография-шифр-виженера-программ/

5. ხუციშვილი ო.,ხუციშვილი თ., ფაილოძე ნ., კაიშაური. თ., ქაშიაშვილი ზ. (2005). ინფორმატიკა, ნაწ.1, სტუ, თბილისი.

ON THE METHODS OF SYMMETRIC CRYPTOGRAPHY In MS Excel ENVIRONMENT

Narishelashvili Gulbaat, Kekelia Valerian, Didmanidze Ibraim

Georgian Technikal Universiti

Summary

On the basis of known cryptographic techniques (Caesar Vizhinera, Vernal, and the inverse matrix) for a symmetrical cryptographic system developed and practically implemented in the medium MS Exel algorithms for encryption / decryption of text information. This allows User The telyam easy to imagine the procedure encryption / decryption, to exchange information with each other (Short text messages), in other words, to communicate in, "cryptographic language".

О РЕАЛИЗАЦИИ МЕТОДОВ СИМЕТРИЧНОЙ СИСТЕМЫ КРИПТОГРАФИИ В СРЕДЕ MS Excel

Нарешелашвили Г., Кекелия В., Дидманидзе И.

Грузинский Технический Университет

Резюме

На базе известных методов криптографии (Цезаря, Вижинера, Вернана и обратной матрицы) для симметричной криптографической системы разработаны и практически реализованы в среде MS Exel алгоритмы шифрации/дешифрации текстовой информации. Это дает возможность пользователям легко представить процедуры шифрации /дешифрации, обменяться между собой информацией (короткими текстовыми сообщениями), иначе говоря , общаться на ,»криптографическом языке».