Scientific and Practical Cyber Security Journal (SPCSJ) 2(1):48-59
Scientific Cyber Security Association (SCSA), 2018 ISSN: 2587-4667

HYBRID ENCRYPTION MODEL OF SYMMETRIC AND ASYMMETRIC CRYPTOGRAPHY WITH AES AND ELGAMAL ENCRYPTION ALGORITHMS

E.Jincharadze
Georgian Technical University, Tbilisi, Georgia

ABSTRACT. Cryptography is the science or study of the techniques of secret writing, especially code and cipher systems, methods, and the like. Cryptography must ensure the high-level security of transferring and saving data. There are two types of cryptography algorithms such as symmetric key cryptography and asymmetric key cryptography. Nowadays there are various types of cryptographic algorithms which provides high security of information, but they also have some weak points too.

To improve weakeness of these algorithms, in this paper we propose a new hybrid cryptographic algorithm model. This algorithm is designed using combination of two cryptographic algorithms AES and Elgamal.

Was done analyses and comparision of the performance of proposed algorithms by following parameters encryption time, decryption time and system requirements.

For this cryptography algorithms were created program on Java in NetBeans IDE. Implementation and performance analysis of this proposed models were done by Java. As a final result shows the hybrid model has better performance than AES and Elgamal systems.

რეზიუმე. კრიპტოგრაფია ეს არის მონაცემთა გადაცემის მეთოდი, რომელიც უზრუნველყოფს გადაცემული ინფორმაციის უსაფრთხოებას. არსებობს ორი სახის კრიპტოგრაფიული ალგორითმები, სიმეტრიულ და ასიმეტრიული გასაღებიანი კრიპტოგრაფია. დღესდღეობით გვაქვს სხვადასხვა სახის კრიპტოგრაფიული ალგორითმები, რომლებიც გვთავაზობენ უსაფრთხოების საკმაოდ მაღალ დონეს, თუმცა თანამედროვე ტექნოლოგიების განვიარებასთან ერთად ამ ალორითმებში ჩნდება სუსტი მხარეები და ნაკლოვანებები. არსებული ნაკლოვანებების გასაუმჯობესებლად მოცემულ ნაშრომში განხილულია ჰიბრიდული კრიპოსისტემა, რომელიც გულისხმობს სიმეტრიული და ასიმეტრიული კრიპტოსისტემის კომბინაციით ახალი სისტემის მიღებას. მოცემული ნაშრომი ასახავს თეორიული/ექსპერიმენტული კვლევის სხვადასხვა ეტაპებს და დასაბუთებულ შედეგებს. წარმოდგენილი და გამოკვლეულია სიმეტრიული და ასიმეტრიული ალგორითმების ზოგადი მიმოხილვა, მათი სუსტი და ძლიერი მხარეები. განხილულია მოცემული ალგორითმების უსაფრთხოების ნორმები. ჩატარებული კვლევების საფუძველზე მიღებული შედეგების გათვალისწინებით შექმნილია ჰიბრიდული კრიპტოსისტემის მოდელი, რომელიც ითვალისწინებს AES და ElGamal სისტემის კომბინაციას. მოცემული კრიპტოსისტემების ალგორითმების საფუძველზე შექმნილია და წარმოდგენილია პროგრამული კოდის რეალიზაცია ობიექტზე ორიენტირებული პროგრამირების ენის JAVA პლატფორმაზე. მოცემული

პროგრამული პროდუქტის საშუალებით ჩატარებულია ცდები აღნიშნული ალგორითმებისა და მათი კომბინაციით შექმნილი ალგორითმის ეფექტურობაზე, რაც ითვალისწინებს ალგორითმის უსაფრთხოების დონის პარამეტრებს, ალგორითმის დამუშავების დროს, დეშიფრაცია/შიფრაციის დროს და ალგორითმის მიმდინარეობის პროცესში კომპიუტერული რესურსების გამოყენების მახასიათებლებს.

KEYWORDS: cryptography, encryption, assymmmetric cryptography, Elgamal;

შესავალი

კრიპტოგრაფია ეს არის მეცნიერება ინფორმაციის საიდუმლოდ და უსაფრთხოდ შენახვისა და გავრცელების შესახებ. ზოგადად კრიპტოგრაფის იყოფა ორ მიმართულებად სიმეტრიულ გასაღებიან და ასიმეტრიულ გასაღებიან კრიპტოსისტემებად.

ასიმეტრიული (საჯარო გასაღებიანი) კრიპტოგრაფის სხვადასხვა ალგორითმები კრიპტოგრაფიის ერთ-ერთ მნიშვნელოვან მიმართულებად ჩამოყალიბდა. ამ ფაქტს განსაკუთრებით ხელს უწყობს გასაღების გავრცელების განსხვავებული ტექნოლოგია. ასიმეტრიული კრიპტოგრაფია შეიცავს ციფრულ ხელმოწერებს, რომლებიც მომხმარებლებს გასაღების ციფრული ხელმოწერით აღჭურვის საშუალებას აძლევს, რაც თავის მხრივ მომხმარებლის იდენტიფიკაციისა და უნიკალურობის დასადგენად საუკეთესო საშუალებაა.

კრიპტოგრაფიული ალგორითმის თვისებას დაიცვას ინფორმაცია სხვადასხვა თავდასხისაგან ალგორითმის სიძლიერე წარმოადგენს. ალგორითმის სიძლიერე დამოკიდებულია სხვადასხვა ფაქტორზე: გასაღების საიდუმლოება; გასაღების გამოცნობის ან სავარაუდო გასაღებების სიხშირის კრიპტოანალიზის სირთულე. ზოგადად რაც უფრო გრძელია გასაღები, მით უფრო რთულია მისი კრიპტოანალიზი; შიფრაციის გასაღების გარეშე ალგორითმის გატეხვის სირთულე; ალგორითმის გატეხვის სხვა სავარაუდო გზების არარსებობა, ან ნაკლებობა;

ზოგადად, კრიპტოგრაფიული ალგორითმის სიძლიერე არ შეიძლება იყოს ბოლომდე უზრუნველყოფილი. რათქმაუნდა ყველა კრიპტოგრაფიული ალგორითმი შექმნილია, როგორც სრულყოფილი და მდგრადი სხვადასხვა თავდასხმის მიმართ, მაგრამ დროთა განმავლობაში ტექნოლოგიური განვითარების და სხვადასხვა ფაქტორების გათვალიწინებით ყველა ალგორითმი დაუცველი ხდება სხვადასხვა თავდასხმის წინაშე.

სიმეტრიული და ასიმეტრიული სისტემების ძლიერი და სუსტი მხარეები

სიმეტრიულ (საიდუმლო გასაღებიან) კრიპტოგრაფიაში ყველა მომხმარებლისთვის გამოყენებულია ერთიდაიგივე კრიპტოგრაფიული გასაღები შიფრაციისა და დეშიფრაციის წარმოებისთვის. [1, 2]. ამ სისტემაში აუცილებელია რომ გამგზავნი და მიმღები წინასწარ შეთანხმდნენ საიდუმლო გასაღების შესახებ. სიმეტრიული ალგორითმის მთელი უსაფრთხოება გასაღებზეა დამოკიდებული.

სიმეტრიული კრიპტოგრაფიის ერთ-ერთ ***ძლიერ მხარეს*** წარმოადგენს შიფრაცია / დეშიფრაციის პროცესში გამოყენებული საიდუმლო გასაღების მდგრადობა უხეში ძალის მეთოდის (Brute Force Attack) წინააღმდეგ. როდესაც ის უსაფრთხო ალგორითმს იყენებს, სიმეტრიული შიფრაცია შეიძლება იყოს ძალიან უსაფრთხო. (ცხრილი 1).

გასაღების სიგრძე	**1 წამში მოძიებული გასაღების რაოდენობა**	**გასაღების ძიების დროს გამოყენებული ტექნიკური რესურსი**	**ყველა გასაღების ძიების სავარაუდო დრო**
40 ბიტი	10	10 წლის დესკტოპ კომპიუტერი	3484 წელი
40 ბიტი	1 მილიარდი	საშუალო ზომის კორპორატიული ქსელი	18 წუთი
56 ბიტი	100 მილიარდი	ტექნოლოგია DES ალგორითმის დეშიფრაციისთვის	8 დღე
64 ბიტი	1 მილიარდი	საშუალო ზომის კორპორატიული ქსელი	585 წელი
128 ბიტი	1×10^{23}	სპეციალური დანიშნულების კვანტური კომპიუტერი 2015 წლის მონაცემებით	108 მილიონი წელი
192 ბიტი	1 მილიარდი	საშუალო ზომის კორპორატიული ქსელი	2×10^{41} წელი
192 ბიტი	1 მილიარდი	დიდი ზომის ინტერნეტ პროექტი 2005 წლის მომნაცემებით	2×10^{32} წელი
192 ბიტი	1×10^{23}	სპეციალური დანიშნულების კვანტური კომპიუტერი 2015 წლის მონაცემებით	2×10^{27} წელი
256 ბიტი	1×10^{23}	სპეციალური დანიშნულების კვანტური კომპიუტერი 2015 წლის მონაცემებით	3.7×10^{46} წელი
256 ბიტი	1×10^{32}	სპეციალური დანიშნულების კვანტური კომპიუტერი 2015 წლის	3.7 x

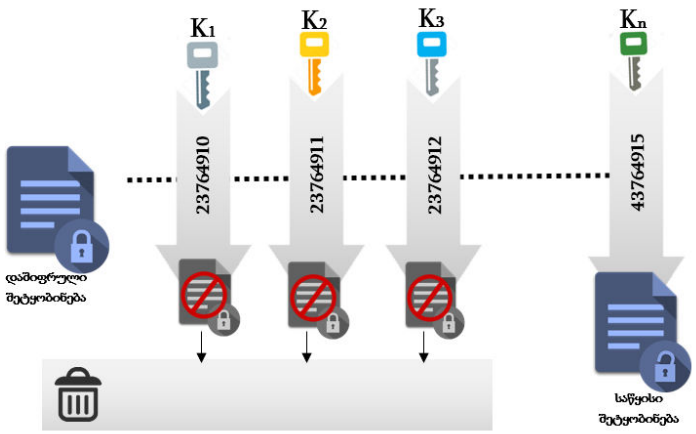
		მონაცემებით	10^{37} წელი

ცხრილი 1. *- უხეში ძალის მეთოდის (brute force) სავარაუდო წარმატების ცხრილი, რომელიც ითვალისწინებს გასაღებებს სხვადასხვა ბიტის ზომის სიგრძით და 1 წამში მოძიებული გასაღების რაოდენობებს.*

ცხადია, რომ დღევანდელი კომპიუტერული სისტემების ტექნიკური შესაძლებლობების გათვალისწინებით არ გვაქვს საჭიროება გამოვიყენოთ 128 ბიტზე გრძელი გასაღებიანი სისტემა. თუმცა, ერთგვარი მარკეტინგული პროცესის შედეგია, რომ უპირატესობა ენიჭება უფრო და უფრო მაღალი გასაღების სიგრძეს. მაგალითად, Rijndael ალგორითმი იყენებს 128-ბიტი, 192-ბიტი, ან 256-ბიტიან გასაღებს.

სიმეტრიული კრიპტოსისტემების ***სუსტ მხარეს*** წარმოადგენს ის ფაქტი თუ რამდენად სწორადაა არჩეული გასაღები.[2]. სიმეტრიული კრიპტოსისტემების წინააღმდეგ გამოიყენება შემდეგი მეთოდები: თავდასხმა უხეში ძალის მეთოდით (brute force), კრიპტოანალიზი, სისტემაზე დაფუძნებული შეტევა.

გასაღების სიგრძის ზრდასთან ერთად ექსპონენციალურად იზრდება შესაძლო პერმუტაციებისრაოდენობა, შესაბამისად იზრდება უხეში ძალით შეტევისათვის საჭირო რესურსების ოდენობა. ასეთი სისტემა გასაღების ძიების სისტემის, ან იგივე შეტევა უხეში ძალის სახელით არის ცნობილი. ნახაზი 1.



ნახაზი 1. *თავდასხმა უხეში ძალის მეთოდით (brute force)*

ასიმეტრიულ (საჯარო გასაღებიანი) კრიპტოგრაფიაში წარმოდგენილია იდეა ისეთი შიფრაციის სისტემის შექმნის შესახებ, სადაც გამოიყენება ორი გასაღები: საჯარო და საიდუმლო. საჯარო გასაღები გამოიყენება შიფრაციისთვის, ხოლო საიდუმლო გასაღები დეშიფრაციისთვის. ამასთან ეს გასაღებები არ უკავშირდებიან ერთმანეთს. ასიმეტრიული კრიპტოგრაფიის მეთოდის უპირველეს ***ნაკლს*** გასაღების მართვის აუცილებლობა წარმოადგენს. ქსელში ყოველ სხვადასხვა წყვილს უწევს იქონიოს ცალკე

გასაღები, რაც წყვილთა რაოდენობის გაზრდისას გასაღებების რაოდენობის კვადრატული პროპორციით გაზრდას იწვევს.

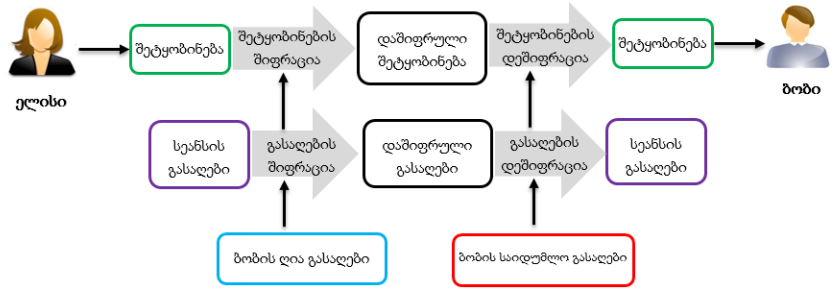
ჰიბრიდული კრიპტოსისტემები

კრიპტოგრაფიაში ჰიბრიდული კრიპოსისტემად ზოგადად მოიხსენიება სისტემა, რომელიც წარმოადგენს ასიმეტრიული და სიმეტრიული შიფრაციის ალგორითმების კომბინაციას. ჰიბრიდული კრიპტოსისტემა ძირითადად წარმოდგენილია შემდეგი სქემის სახით:

- გასაღების ენკაფსულაციის სქემა, გამოიყენება საჯარო გასაღებიანი, ასიმეტრიული კრიპტოსისტემა;
- მონაცემთა ენკაფსულაციის სქემა, გამოიყენება ფარულ გასაღებიანი, სიმეტრიული კრიპტოსისტემა;

ღია გასაღების კრიპტოსისტემები დაფუძნებულია რთული პრობლემების გამოთვლით სირთულეზე. მაგალითად RSA ემყარება რიცხვის ფაქტორიზაციის პრობლემას (ანუ დიდი რიცხვის დაშლას მარტივ მამრავლებად). მსგავსი სისტემების შემთხვევაში უპირატესობა ენიჭება მოდულით გამრავლების და ახარისხების ოპერაციებს, შესაბამისად გაცილებით მეტი გამოთვლითი სიმძლავრეა საჭირო, ვიდრე სიმეტრიულ სისტემებში. ამიტომ ღია გასაღების კრიპტოსისტემები ძირითადად გამოიყენება, როგორც ჰიბრიდული სისტემები, სადაც ინფორმაციის შიფრაცია/დეშიფრაციისათვის გამოიყენება სწრაფი სიმეტრიული ალგორითმები, ხოლო მისი გასაღების მართვისა და გადაცემისათვის გამოიყენება შედარებით ნელი ასიმეტრიული ალგორითმები.

როგორც აღვნიშნეთ, სიმეტრიულ და ასიმეტრიულ ალგორითმებს გააჩნია თავისი დადებითი და უარყოფითი მხარეები. სიმეტრიული ალგორითმების სისტემები არიან საკმაოდ სწრაფი, ვიდრე ასიმეტრიული სისტემები, თუმცა მოითხოვს რომ ფარული გასაღები დაცულად იქნეს გადაცემული შიფრაციის სქემის მეორე მხარისთვის. ხოლო ასიმეტრიული სისტემები უზრუნველყოს ღია გასაღების გაცვლას და საიდუმლო გასაღების უსაფრთხოების დაცვას, თუმცა ეს ხდება სისწრაფის ხარჯზე. სწორედ, ამ პრობლემების აღმოფხვრის მიზნით გამოიყენება ჰიბრიდული ალგორითმები, რაც გულისხმობს შიფრაციის პროცესში სხვადასხვა ტიპის ალგორითმების გამოყენებას. ამსისტემი ზოგადი იდეა მდგომარეობს იმაში, რომ მოვახდინოთ შემთხვევითი გასაღების გენერირება სიმეტრიული შიფრაციისთვის, ხოლო შემდეგ მოვახდინოთ ამ გასაღების შიფრაცია ასიმეტრიული სისტემისათვის. შემდეგ მიღებული საიდუმლო გასაღებით ხდება საწყისი შეტყობინების შიფრაცია. დეშიფრაციის დროს ხდება შეტყობინების დაშიფვრა საკუთარი საიდუმლო გასაღებით, ხოლო შემდეგ გამოყენება საჯარო გასაღები. ნახაზი 2.



ნახაზი 2. *ჰიბრიდული კრიპტოსისტემის ზოგადი სქემა*

მოცემულ სქემაზე განიხილება შემდეგი კომბინაცია: ელისი აგზავნის შეტყობინებას, ხოლო ადრესატი არის ბობი. შეტყობინება უნდა გაიგზვნოს დაშიფრული სახით, უსაფრთხსოების წესების გათვალისწინებით.

AES - განვითარებული შიფრაციის სტანდარტი

AES იგივე Rijndael წარმოადგენს სიმეტრიული შიფრაციის ალგორითმს. მუშაობს მხოლოდ 128 ბიტიან ბლოკებთან მაშინ როცა Rijndael წარადგენს ბლოკების ზომებს და 32-ის ჯერად გასაღებებს (128-ს და 256 შორის).[2, 3]. ალგორითმი იღებს დასაწყისში 128 ბიტიან (16 ბაიტი) ბლოკს, გასაღები მოიცავს 128, 192 ან 256 ბიტს. დასაწყისის 16 ბაიტი არის გადაადგილებული წინასწარ განსაზღვრული ცხრილის მიხედვით. AES ალგორითმზე თავდასხმებში ყველაზე ეფექტურად და სწრაფად უხეში ძალის მეთოდი მიიჩნევა. თუმცა 2013 წლამდე არც-ერთი მათგანი არ მიიჩნეოდა შესაძლებლად. AES - 128 -თვის გასაღები შეიძლება აღდგეს $2^{126,1}$ გამოთვლითი სირთულით.

ElGamal კრიპტოსისტემა

მოცემული სისტემა წარმოადგენს ასიმეტრიულ კრიპტოგრაფიულ ალგორითმს, რომელიც არის RSA ალგორმითმის ალტერნატივა და მისგან განსხვავებით ეყრდნობა დისკრეტული ლოგარითმის პრობლემას. ალგორითმი გვთავაზობს უსაფრთხოების დამატებითი ნორმების მხარდაჭერას, რაც მდგომარეობს ამ სისტემაში სიმეტრიული ალგორითმით დაშიფრული შეტყობინების ასიმეტრიული ალგორითმით დაშიფრული გასაღებით შიფრაციას [16]. ელგამალის სისტემაში შიფრაცია / დეშიფრაციის პროცესი იყო სამ ეტაპად: გასაღების გენერირება; საწყისი შეტყობინების შიფრაცია; დაშიფრული შეტყობინების დეშფრაცია.

თავდაპირველად ხდება გასაღების გენერირება, ამ დროს გვაქს შემდეგი ეტაპები[16]:

- ელისი აგენერირებს შემთხვევით მარტივ რიცხვს p ;

- შემდეგში ხდება ისეთი g გენერატორის შერჩევა, რომელიც აკმაყოფილებს პირობას $g < p$;
- ელისი შემთხვევითად ირჩევს ისეთ მთელ x რიცხვს, რომელიც აკმაყოფილებს შემდეგ პირობას $1 < x < p$;
- ხდება $y = g^x \ mod \ p$ გამოსახულების გამოთვლა;
- ელისი მოცემული მოქმედებების შედეგად მიღებულ პარამეტრებიდან y, g და p გაუგზავნის ბობს, როგორც ღია გასაღებებს, ხოლო x წარმოადგენს ელისის ფარულ გასაღებს, რომელსაც საიდუმლოდ ინახავს.

ელგამალ ალგორითმის მეორე ეტაპია შეტყობინების შიფრაცია. მას შემდეგ, რაც ბობი ღებულობს ღია გასაღებებს ელისისგან იწყებს შეტყობინების დაშიფვრას ამ გასაღებების გამოყენებით. გვაქვს შემდეგი ეტაპები [16]:

- თავდაპირველად გვაქვს საწყისი M შეტყობინება. ბობი ირჩევს შემთხვევით k გასაღებს სესიისთვის. შერჩეული k გასაღები წარმოადგენს ისეთ მთელ რიცხვს, რომელიც აკმაყოფილებს პირობას $1 < \ k \ < p - 1$;
- შემდეგში ხდება a და b რიცხვების გამოთვლა, სადაც $a = \ g^k \ mod \ p$, ხოლო $b = y^k M \ \ mod \ p$;
- სწორედ მიღებული (a, b) წარმოადგენს დაშიფრულ შეტყობინებას.

დეშიფრაცია - ელისი თავისი საიდუმლო გასაღების გამოყენებით მოახდენს ბობის მიერ დაშიფრული შეტყობინების დეშიფრაციას. დეშფრაციის დროს გვაქვს შემდეგი პროცესი:

- იმისათვის, რომ მივიღოთ საწყისი M შემტყობინება, ელისი ასრულებს შემდეგი გამოსახულების გამოთვლას, სადაც გამოიყენებს თავის საიდუმლო x გასაღებს $M = b \ (a^x)^{-1} \ \ mod \ \ p$

ელგამალ ალგორითმის უსაფრთხოების უზრუნველსაყოფად გამოიყენება სხვადასხვა სიგრძის შემთხვევითი k გასაღები. ალგორითმის *უარყოფით* მხარეს წარმოადგენს საწყის შეტყობინებასთან შედარებით დაშიფრული შეტყობინების გაორმაგებული სიგრძე. ელგამალ ალგორითმის უსაფრთხოების მიზნით ასევე აუცილებელია, ყოველი M და M' სხვადასხვა შეტყობინების შიფრაციის დროს გამეყენებული იქნას სხვადასხვა k გასაღები. წინააღმდეგ შემთხვევაში, თუ გამოყენებული იქნება ერთიდაიგივე k გასაღები მაშინ შესაბამისი შიფროტექსტები იქნება შემდეგი (a, b) და (a', b'), რომლებისთვისაც სრულდება შემდეგი პირობა $b(b')^{-1} = M(M')^{-1}$. მოცემული გამოსახულებიდან მარტივადაა შესაძლებელი M' გამოთვლა, თუ ცნობილია M.

დღესდღეობით ღია გასაღებიანი კრიპტოგრაფიული სისტემები პერსპექტიულ სისტემებად ითვლებიან.

AES და ELgamal სისტემების პროგრამული რეალიზაცია

AES და ELgamal კრიპტოსისტემებზე პროგრამული ექსპერიმენტების ჩატარების, მაქსიმალური გამოყენების დროის, გამოყენებული მეხსიერების შედეგების კვლევის მიზნით შეიქმნა მოცემული სისტემების ალგორითმების პროგრამული რეალიზაცია. ამ მიზნით გამოყენებული JAVA ობიექტზე ორიენტირებული პროგრამირების ენა. თუმცა გამოთვლების სტატისტიკური შედეგების სიზუსტის მიზნით გამოყენებულია არა ვიზუალური ინტერფეისით, არამედ პროგრამასთან კონსოლური მუშაობის რეჟიმი.

განხილული პროგრამული კოდის გამოყენებით ჩატარდა ექსპერიმენტული კვლევა. კვლევაში გამოყენებული იქნა კომპიუტერი შემდეგი ტექნიკური და პროგრამული მახასიათებლებით (ცხრილი 2):

ოპერაციული სისტემა	Windows 10
პროცესორი	Intel Core i7-7500U up to 3.5 Ghz
ოპერატიული მეხსიერება	8GB DDR4
ვიდეო დაფა	Nvidia GeForce 940MX 2GB

ცხრილი 2. *სისტემური და პროგრამული მახასიათებლები*

ზოგადად შიფრაციის სრული დრო უმთავრესად დამოკიდებულია კონკრეტული ალგორითმის სტრუქტურულ მახასიათებლებზე. ცხრილ 3-ში მოცემულია სხვადასხვა ზომის დასაშიფრი ტექსტზე ჩატარებული შიფრაციისა და დეშიფრაციის ოპერაციები AES კრიპტოსისტემის გამოყენებით.

AES შიფრაცია				
დასაშიფრი ტექსტის ზომა	**გასაღების ზომა**	**შესრულების დრო**	**გამოყენებული მეხსიერება**	**დაშიფრული ტექსტის ზომა**
32 ბიტი	16 ბიტი	3808063804 ნანოწამი	10766672 ბიტი	64 ბიტი
256 ბიტი	16 ბიტი	2295256727 ნანოწამი	10779768 ბიტი	364 ბიტი
512 ბიტი	16 ბიტი	2146070146 ნანოწამი	10773712 ბიტი	728 ბიტი
1024 ბიტი	16 ბიტი	1753139003 ნანოწამი	10773560 ბიტი	1388 ბიტი
8192 ბიტი	16 ბიტი	2115241833 ნანოწამი	10776936 ბიტი	10944 ბიტი
65032 ბიტი	16 ბიტი	10367833926 ნანოწამი	12898992 ბიტი	87404 ბიტი
AES დეშიფრაცია				

გასაშიფრი ტექსტის ზომა	გასაღების ზომა	შესრულების დრო	გამოყენებული მეხსიერება	დაშიფრული ტექსტის ზომა
64 ბიტი	16 ბიტი	10468516 ნანოწამი	107666724 ბიტი	32 ბიტი
364 ბიტი	16 ბიტი	2751477 ნანოწამი	107797688 ბიტი	256 ბიტი
728 ბიტი	16 ბიტი	2791322 ნანოწამი	107737128 ბიტი	512 ბიტი
1388 ბიტი	16 ბიტი	5015988 ნანოწამი	107735608 ბიტი	1024 ბიტი
10944 ბიტი	16 ბიტი	25160336 ნანოწამი	11448024 ბიტი	2000 ბიტი
87404 ბიტი	16 ბიტი	79623559 ნანოწამი	14315344 ბიტი	5000 ბიტი

ცხრილი 3. *AES შიფრაცია / დეშიფრაციის სტატისტიკური მაჩვენებლები*

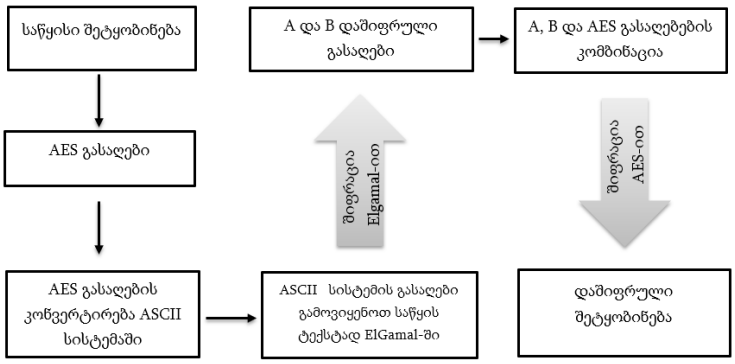
მსგავსი სახის ექსპერიმენტი ჩატარდა ასევე Elgamal კრიპტოსისტემაზე. შედეგად მივიღეთ შემდეგი მონაცემები (ცხრილი 4):

Elgamal შიფრაცია		
მონაცემის ზომა	**დრო**	**გამოყენებული მეხსიერება**
32 ბიტი	5489281831 ნანოწამი	4027936 ბიტი
64 ბიტი	7432850294 ნანოწამი	4027096 ბიტი
512 ბიტი	25335174821 ნანოწამი	7388952 ბიტი
1024 ბიტი	40615441061 ნანოწამი	11409872 ბიტი
Elgamal დეშიფრაცია		
32 ბიტი	1403419 ნანოწამი	4027936 ბიტი
64 ბიტი	2290604 ნანოწამი	4027096 ბიტი
512 ბიტი	10499547 ნანოწამი	7388952 ბიტი
1024 ბიტი	9428294 ნანოწამი	12080984 ბიტი

ცხრილი 4. Elgamal კრიპტოსისტემის შიფრაცია / დეშიფრაცია

AES და ELgamal კრიპტოსისტემების შედეგად შექმნილი ჰიბრიდული სისტემა

განვიხილოთ ჰიბრიდული კრიპტოსისტემა, რომელიც ზემოთ განხილული AES და ELgamal კრიპტოსისტემების კომბინაციის საფუძველზე არის შექმნილი. თავდაპირველად ხდება AES და Elgamal საიდუმლო გასაღების შეყვანა. ხდება შეყვანილი AES გასაღების კონვერტირება შესაბამის ASCII რიცხვების სისტემაში. კონვერტირებული გასაღები გამოყენება Elgamal გასაღების შიფრაციისთვის. დაშიფრული გასაღების A შიფროტექსტითა და AES გასაღების კომბინაციით ხდება საწყისი შეტყობინების შიფრაცია AES შიფრაციის სქემით. დეშიფრაცია ხდება შებრუნებული მიმდევრობით (ნახაზი 3).

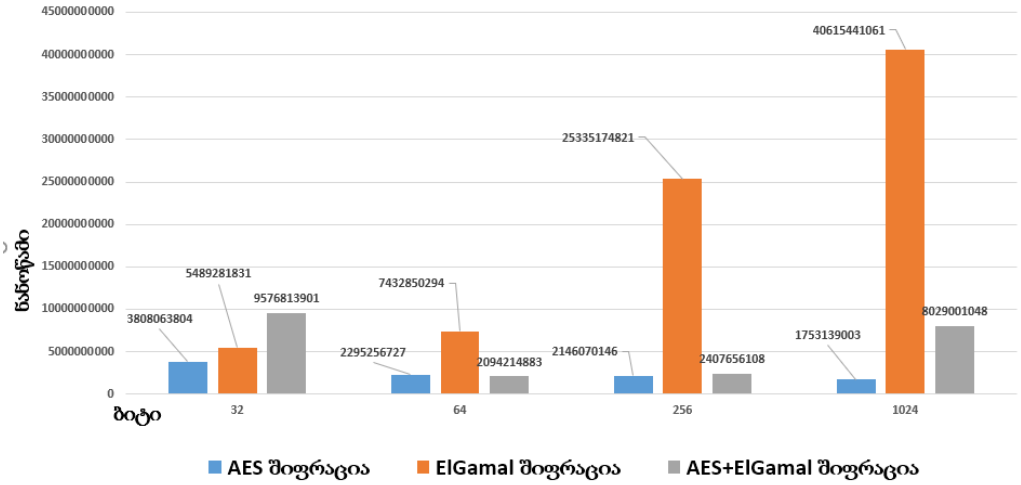


ნახაზი 3. *AES + ElGamal კრიპტოსისტემების კომბინაციით მიღებული ჰიბრიდული კრიპოსისტემის ზოგადი არქიტექტურა*

მოცემული სისტემის ალგორითმის Java პლატფორმაში რეალიზებული პროგრამული კოდის გამოყენებით შესრულდა სხვადასხვა ზომის მონაცემებზე შიფრაციისა და დეშიფრაციის პროცესები. (ცხრილი 5).

AES + Elgamal შიფრაცია		
მონაცემის ზომა	**დრო**	**გამოყენებული მეხსიერება**
32 ბიტი	9576813901 ნანოწამი	11466368 ბიტი
64 ბიტი	2094214883 ნანოწამი	11451128 ბიტი
256 ბიტი	2407656108 ნანოწამი	11473608 ბიტი
1024 ბიტი	8029001048 ნანოწამი	11466272 ბიტი
AES + Elgamal დეშიფრაცია		
32 ბიტი	5197938 ნანოწამი	11450432 ბიტი
64 ბიტი	4874588 ნანოწამი	11450432 ბიტი
256 ბიტი	5160914 ნანოწამი	11450432 ბიტი
1024 ბიტი	6209952 ნანოწამი	11450432 ბიტი

ცხრილი 5. *AES + Elgamal შიფრაცია/დეშიფრაციის სტატისტიკური მაჩვენებლები*



სურათი 6. *განხილულ სისტემებში საწყისი მონაცემების (ბიტი) შიფრაციისა და დროის (ნანოწამი) დამოკიდებულების გრაფიკი*

დასკვნა

მონაცემთა უსაფრთხოების მიზნით გამოიყენება სხვადასხვა კრიპტოგრაფიული ალგორითმები. მათ ერთ-ერთ უპირატესობას პროცესის სისწრაფე და კრიპტოთავდასხმის წინააღმდეგ მაღალი მდგრადობა განაპირობებს. მოცემულ ნაშრომში განხილულია ორი სხვადასხვა სისტემის: სიმეტრიული AES და ასიმეტრიული ElGamal ალგორითმის პროგრამული რეალიზაცია Java პროგრამირების ენაზე. წარმოდგენილია მოცემული ორი ალგორთმის კომბინაციით მიღებული ჰიბრიდული ალგორითმი და ასევე მისი პროგრამული რეალიზაცია. მოცემულ ალგორითმებზე ჩატარდა ექსპერიმენტები, რაც ითვალისწინებდა სხვადასხვა ზომის საწყისი მონაცემის შიფრაცია/დეშიფრაციის პროცესების შესრულება სამივე ალგორითმზე. შედეგად ძირითადი დაკვირვების ობიექტს წარმოადგენდა მათი შესრულების დრო და მოხმარებული მეხსიერების მაჩვენებელი. როგორც ჩატარებული ექსპერიმენტები გვიჩვენებს, რომ განხილული ჰიბრიდული ალგორითმი არის უფრო სწრაფი და ამავდროულად უსაფრთხო რადგან გათვალისწინებულია, როგორც სიმეტრიული ასევე ასიმეტრიული ალგორითმის ძლიერი მხარეები.

მოცემულ ნაშრომში განხილული საკითხის შემდგომ გაგრძელებად შესაძლებელია განხილული იქნას სხვა სიმეტრიული და ასიმეტრიული ალგორითმის ჰიბრიდული მოდელი, რომლისთვისაც წარმოდგენილი და გაანალიზებული იქნება სტრუქტურა, უსაფრთხოების დონე, უპირატესობები და ნაკლოვანებები.

REFERENCES

1. Introduction to Cryptography, Second Edition, Johhanes A. Buhman, 2000
2. Handbook of Applied Cryptography, Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanston, Massachusetts Institute of Technology, June 1996
3. Physical Security of Cryptographic Algorithm Implementations, Ilya KIZHVATOV, L'UNIVERSITÉ DU LUXEMBOURG, 2009
4. Ростовцев А. Г., Михайлова Н. В. Методы криптоанализа классических шифров . – М.: Наука, 1995.
5. The official Advanced Encryption Standard" (PDF). Computer Security Resource Center. National Institute of Standards and Technology. Retrieved 26 March 2015.
6. Баричев С. В. Криптография без секретов. – М.: Наука, 1998.
7. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке С, 2-е изд . – М.: Вильямс, 2003.
8. Мао В. Современная криптография: Теория и практика — М.: Вильямс, 2005
9. Ященко В. В. Введение в криптографию. СПб.: Питер, 2001.
10. Introduction to Modern Cryptography by Phillip Rogaway and Mihir Bellare, 2005
11. "An Introduction to Modern Cryptosystems". Andrew Zwicke, 2003
12. "Quantum cryptography: An emerging technology in network security". - Sharbaf, M.S. IEEE International Conference on Technologies for Homeland Security . 2011
13. Adleman, Leonard M.; Rothemund, Paul W.K.; Roweis, Sam; Winfree, Erik (June 10–12, 1996). On Applying Molecular Computation To The Data Encryption Standard. Proceedings of the Second Annual Meeting on DNA Based Computers. Princeton University.
14. Cramer, Ronald; Shoup, Victor (2004). "Design and Analysis of Practical Public-Key Encryption Schemes Secure against Adaptive Chosen Ciphertext Attack"
15. Hofheinz, Dennis; Kiltz, Eike (2007). "Secure Hybrid Encryption from Weakened Key Encapsulation"
16. Taher ElGamal (1985). «A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms