**Scientific and Practical Cyber Security Journal (SPCSJ) 2(4): 40-50 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)**

# BLOWFISH და RSA კრიპტოსისტემების ჰიბრიდული მოდელი

ელზა ჯინჭარაძე
საქართველოს ტექნიკური უნივერსიტეტი

**აბსტრაქტი.** მოცემულ ნაშრომში განხილულია შიფრაციის ცნობილი ორი ალგორითმის RSA (ასიმეტრიული შიფირაციის ალგორითმი) და Blowfish (სიმეტრიული შიფრაციის ალგორითმი) პროგრამული კოდის რეალიზაცია Java პროგრამირების ენის ბაზაზე. ჩატარებული კვლევების საფუძველზე მიღებული შედეგების გათვალისწინებით შექმნილია ჰიბრიდული კრიპტოსისტემის მოდელი, რომელიც ითვალისწინებს RSA და Blowfish სისტემის კომბინაციას და მათი, როგორც ერთი ჰიბრიდული მოდელის პროგრამულ რეალიზაციას.

JAVA პროგრამირების ენაში რეალიზებული 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.

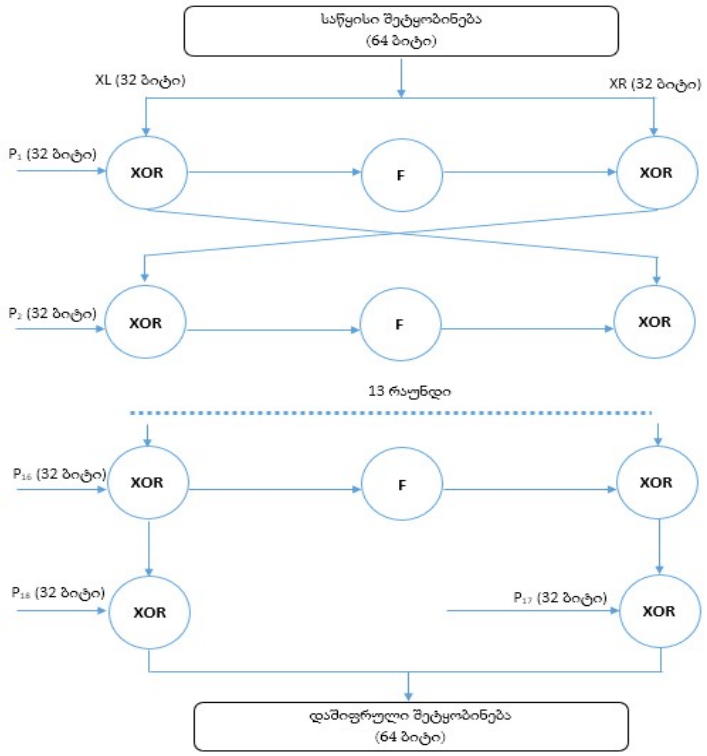
## ასიმეტრიული შიფრაციის ალგორითმების ზოგადი მიმოხილვა RSA კრიპტოგრაფიული ალგორითმის მაგალითზე

ალგორითმი Rivest Shamir Adleman ანუ RSA — კრიპტოგრაფიის ასიმეტრიული ალგორითმი (public სიტყვა-გასაღები), მნიშვნელოვან გამოყენებას ჰპოვებს ელექტრონულ კომერციაში, განსაკუთრებით საიდუმლო მონაცემების გაცვლა-გამოცვლისათვის ინტერნეტში [1,2]. კრიპტოსისტემა RSA წარმოადგენს ღია გასაღებიან ალგორითმს, რომელიც შეიძლება გამოყენებული იქნას როგორც ინფორმაციის დასაშიფრად, ასევე ციფრული ხელმოწერის შესაქმნელად. ალგორითმში ღია და საიდუმლო გასაღებებს შორის დამოკიდებულება მოცემულია ცალმხრივი ფუნქციის საშუალებით. ალგორითმი იყენებს ორი ტიპის სიტყვა-გასაღებს: public, ტექსტის დასაშიფრად და private დაშიფრული ტექსტის გასაშიფრად. public სიტყვა-გასაღები ხელმისაწვდომია ყველასთვის ვინც შიფრავს ინფორმაციას, private კი ხელმისაწვდომია მხოლოდ მისთვის ვინც შექმნა ორივე სიტყვა-გასაღები.

RSA კრიპტოგრაფიული ალგორითმის *უარყოფითი* მხარეა მისი შიფრაციის სიჩქარე. ამ ალგორითმის შიფრაციის პროცესი მოითხოვს საკმაოდ დიდ დროს. ასევე, როგორც სხვა ასიმეტრიული ალგორითმების მსგავსად მთავარ უარყოფით მხარეს წარმოადგენს შიფრაციის პროცესში ორი გასაღების გამოყენების ფაქტი. რა თქმა უნდა RSA გვთავაზობს უსაფრთხოების მაღალ დონეს, მაგრამ ამავდროულად არის საკმაოდ ნელი.

## სიმეტრიული შიფრაციის ალგორითმების ზოგადი მიმოხილვა Blowfish ალგორითმის მაგალითზე

Blowfish წარმოადგენს სიმეტრიული შიფრაცია/დეშიფრაციის კრიპტოგრაფიულ ალგორითმს. მონაცემთა შიფრაციის ფუნქცია საკმაოდ მარტივია. იგი მიმდევრობით 16-ჯერ წარმატებით გამოიყენება ისეთ აპლიკაციებში, სადაც გასაღების სიგრძე პერიოდულად არ იცვლება. ითვლება, რომ არსებულ შიფრაციის ალგორითმებთან შედარებით Blowfish არის უფრო სწრაფი 32 ბიტიან მიკროპროცესორზე შესრულების დროს.



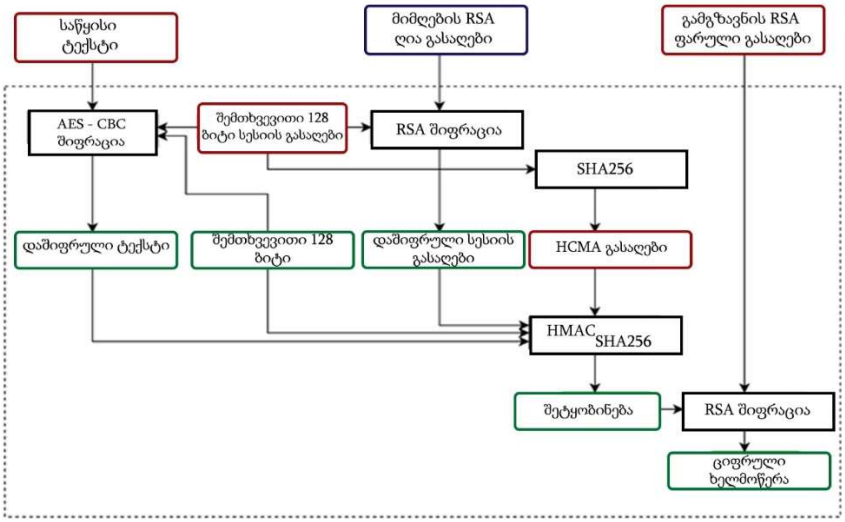

*სურათი 1. Blowfish ალგორითმის სტრუქტურა*

ამ დროისთვის Blowfish გვთავაზობს შედარებით უფრო მაღალი დონის შიფრაციას, რადგან ჯერჯერობით მასზე განხორციელებული არც ერთი შეტევა არ დასრულებულა წარმატებით. Blowfish არის უფრო სწრაფი ვიდრე DES. თუმცა ამ ალგორითმის სუსტი წერტილია შიფრაციის სუსტი გასაღები.

## ჰიბრიდული კრიპტოსისტემების მიმოხილვა

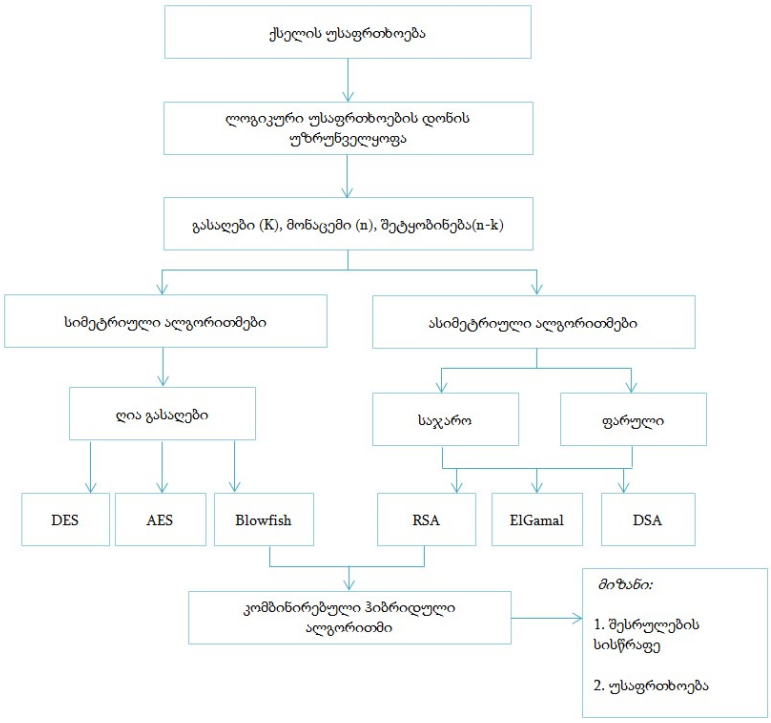
კრიპტოგრაფიაში ჰიბრიდული კრიპოსისტემად ზოგადად მოიხსენიება სისტემა, რომელიც წარმოადგენს ასიმეტრიული და სიმეტრიული შიფრაციის ალგორითმების კომბინაციას [30]. ღია გასაღების კრიპტოსისტემები დაფუძნებულია რთული პრობლემების გამოთვლით სირთულეზე. მაგალითად RSA ემყარება რიცხვის ფაქტორიზაციის პრობლემას (ანუ დიდი რიცხვის დაშლას მარტივ მამრავლებად), ხოლო დიფი-ჰელმანის ალგორითმი ეფუძნება

დისკრეტული ლოგარითმების პრობლემას. 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.




***სურათი 2**. RSA & AES ჰიბრიდული სქემის მოდელი*

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.




*სურათი 3. ჰიბრიდული კრიპტოსისტემის ზოგადი სქემა*

ჰიბრიდული კრიპტოგრაფიული სისტემის 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 [31].

## Blowfish და RSA ალგორითმების პროგრამული რეალიზაცია და ექსპერიმენტული კვლევის შედეგები

Blowfish და RSA 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 ინტერფეისი, არამედ პროგრამასთან კონსოლური მუშაობის რეჟიმი.

ზოგადად შიფრაციის სრული დრო უმთავრესად დამოკიდებულია კონკრეტული ალგორითმის სტრუქტურულ მახასიათებლებზე. ცხრილ 1-ში მოცემულია სხვადასხვა ზომის დასაშიფრი ტექსტზე ჩატარებული შიფრაციისა და დეშიფრაციის ოპერაციები AES

კრიპტოსისტემის გამოყენებით. აქვე უნდა გავითვალისწინოთ, რომ შიფრაციის დროს გამოყენებული გასაღების ზომაა 16 ბიტი.

| Blowfish შიფრაცია | | | | | |
|---|---|---|---|---|---|
| დასაშიფრი ტექსტის ზომა (კილობაიტი) | დასაშიფრი ტექსტის ზომა (ბაიტი) | გასაღების ზომა (ბიტი) | შიფრაციის დრო (ნანოწამი) | დაშიფრული ტექსტის ზომა (ბაიტი) | დეშიფრაციის დრო (ნანოწამი) |
| 32 | 32710 | 16 | 10753053 | 59241 | 1984528 |
| 64 | 65420 | 16 | 12169867 | 119493 | 2743007 |
| 128 | 130840 | 16 | 12567266 | 236670 | 5602025 |
| 256 | 261680 | 16 | 18200673 | 475738 | 9356337 |
| 512 | 523360 | 16 | 23987822 | 954280 | 16802548 |
| 1024 | 1048460 | 16 | 35550482 | 1915678 | 26062972 |
| 2048 | 2096920 | 16 | 43489299 | 3804367 | 40463494 |
| 4096 | 4193840 | 16 | 62097598 | 7552059 | 56950097 |

*ცხრილი 1. Blowfish შიფრაციის სტატისტიკური მაჩვენებლები*

მსგავსი სახის ექსპერიმენტი ჩატარდა ასევე **RSA** კრიპტოსისტემაზე, სადაც სხვადასხვა ზომის ფაილების შიფრაციისა და დეშიფრაციის პროცესზე დახარჯული დროის დაკვირვების შედეგად შედეგად მივიღეთ შემდეგი მონაცემები (ცხრილი 2):

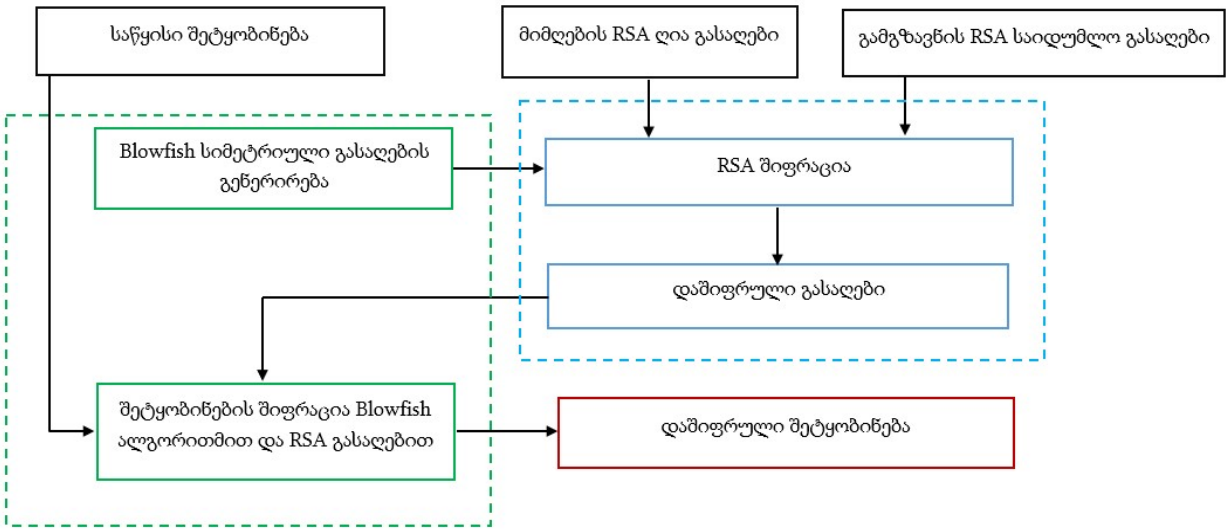
| RSA შიფრაცია | | | | |
|---|---|---|---|---|
| ფაილის ზომა (KB) | საწყისი ფაილის ზომა (Byte) | შიფრაციის დრო (ნანოწამი) | დაშიფრული ტექსტის ზომა | დეშიფრაციის დრო (ნანოწამი) |
| 32 | 32710 | 1536637771 | 118780 | 55542452 |
| 64 | 65420 | 3208498484 | 237689 | 121344997 |
| 128 | 130840 | 6149709140 | 474654 | 284935252 |
| 256 | 261680 | 10574937240 | 946614 | 671696785 |
| 512 | 523360 | 20368096461 | 1896331 | 1991097468 |
| 1024 | 1048460 | 41504791208 | 3795983 | 6934459468 |
| 2048 | 2096920 | 89946149790 | 7586016 | 27974097086 |
| 4096 | 4193840 | 181620236481 | 15179673 | 121238321204 |

*ცხრილი 2. RSA შიფრაციის სტატისტიკური მაჩვენებლები*

## Blowfish + RSA სიმეტრიული და ასიმეტრიული კრიპტოსისტემების შედეგად შექმნილი ჰიბრიდული სისტემა

განვიხილოთ ჰიბრიდული კრიპტოსისტემა, რომელიც ზემოთ განხილული Blowfish და RSA კრიპტოსისტემების კომბინაციის საფუძველზე არის შექმნილი. ამ სისტემის იდეა მდგომარეობს შემდეგში. მოცემული სქემის საწყის ეტაპზე ხდება საწყისი ფაილის წაკითხვა. ამავდროულად ხდება RSA ალგორითმის საიდუმლო და ღია გასაღებების ავტომატური გენერირება.

მოცემული სქემის შემდეგ ეტაპზე ავტომატურად გენერირედება Blowfish სიმეტრიული გასაღები, ხოლო მიღებული გასაღები იშიფრება RSA ალგორითმის საშუალებით. აღნიშნული სქემა უზრუნველყოფს Blowfish სისტემის საჯარო გასაღების უსაფრთხოების მაღალ დონეს. RSA ალგორითმის უსაფრთხოების მაჩვენებელი ამცირებს საჯარო გასაღების დეშიფრაციის რისკებს. შესაბამისად ღია გასაღების გაცვლასთან ერთად მოხდება RSA ალგორითმის საიდუმლო გასაღების გაცვლაც. მოცემულ ჰიბრიდულ მოდელში შიფრაციის პროცესი მიმდინარეობს Blowfish ალგორითმის შიფრაციული ალგორითმით, ვინაიდან Blowfish არის მნიშვნელოვნად სწრაფი, ვიდრე RSA ალგორითმი. შესაბამისად, დეშიფრაციის პროცესი შესრულდება შებრუნებული თანმიმდევრობით.




***სურათი 3.*** *RSA + Blowfish კრიპტოსისტემების კომბინაციით მიღებული ჰიბრიდული კრიპოსისტემის ზოგადი არქიტექტურა*

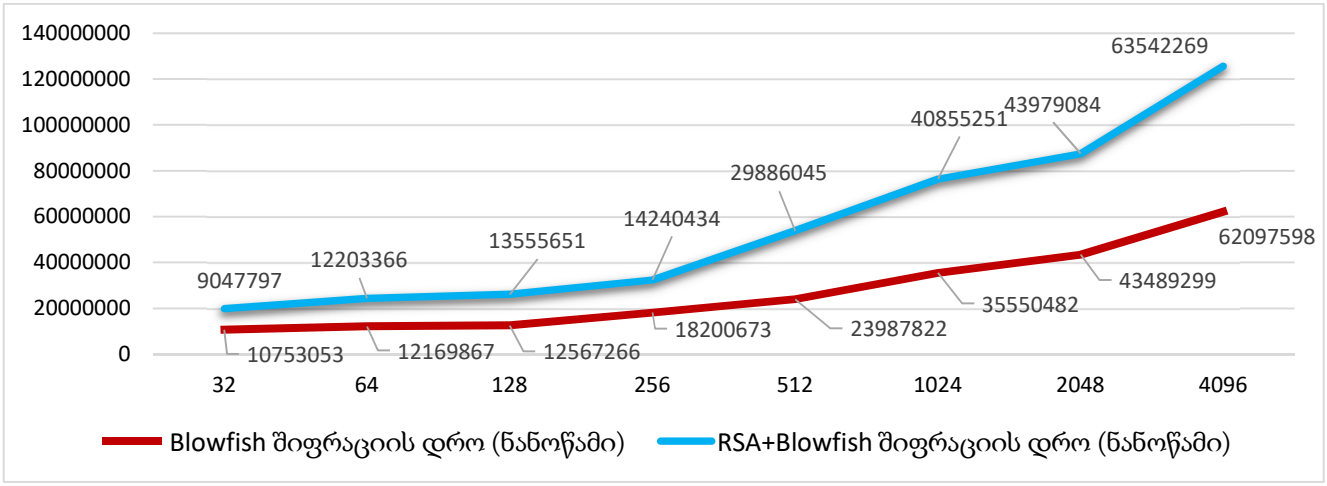
მოცემული სისტემის ალგორითმის Java პლატფორმაში რეალიზებული პროგრამული კოდის გამოყენებით შესრულდა სხვადასხვა ზომის მონაცემებზე შიფრაციისა და დეშიფრაციის პროცესები. (ცხრილი 3).

| Blowfish + RSA შიფრაცია | | | | |
|---|---|---|---|---|
| ფაილის ზომა (KB) | საწყისი ფაილის | შიფრაციის დრო (ნანოწამი) | დაშიფრული ტექსტის ზომა | დეშიფრაციის დრო (ნანოწამი) |

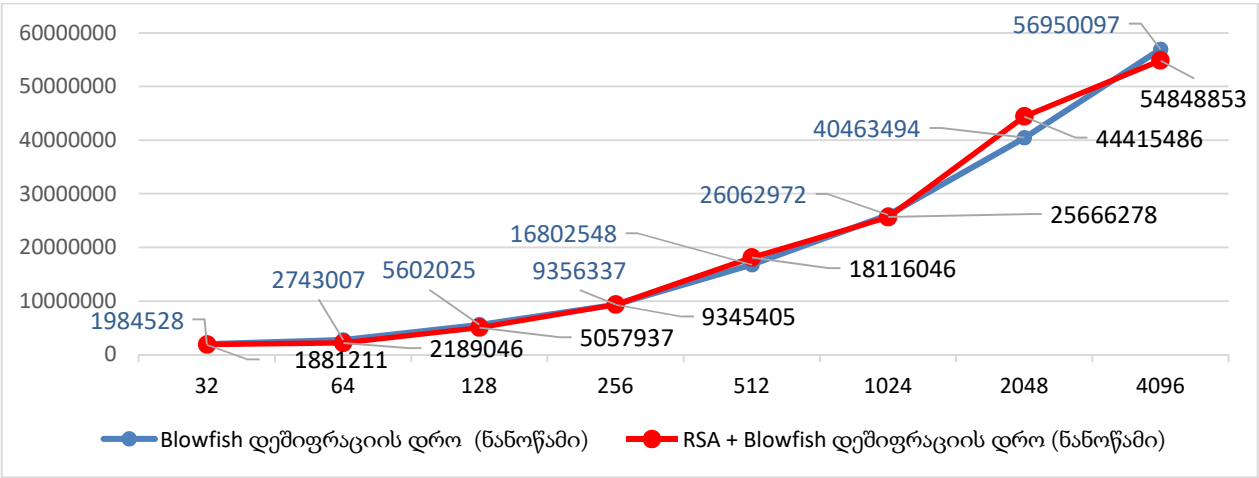
| | ზომა (Byte) | | | |
|---|---|---|---|---|
| 32 | 32710 | 9047797 | 59355 | 1881211 |
| 64 | 65420 | 12203366 | 118428 | 2189046 |
| 128 | 130840 | 13555651 | 237417 | 5057937 |
| 256 | 261680 | 14240434 | 477370 | 9345405 |
| 512 | 523360 | 29886045 | 951418 | 18116046 |
| 1024 | 1048460 | 40855251 | 1898922 | 25666278 |
| 2048 | 2096920 | 43979084 | 3813804 | 54415486 |
| 4096 | 4193840 | 63542269 | 7624638 | 54848853 |

*ცხრილი 3. Blowfish + RSA ჰიბრიდული კრიპტოსისტემის შიფრაციის პროცესი*

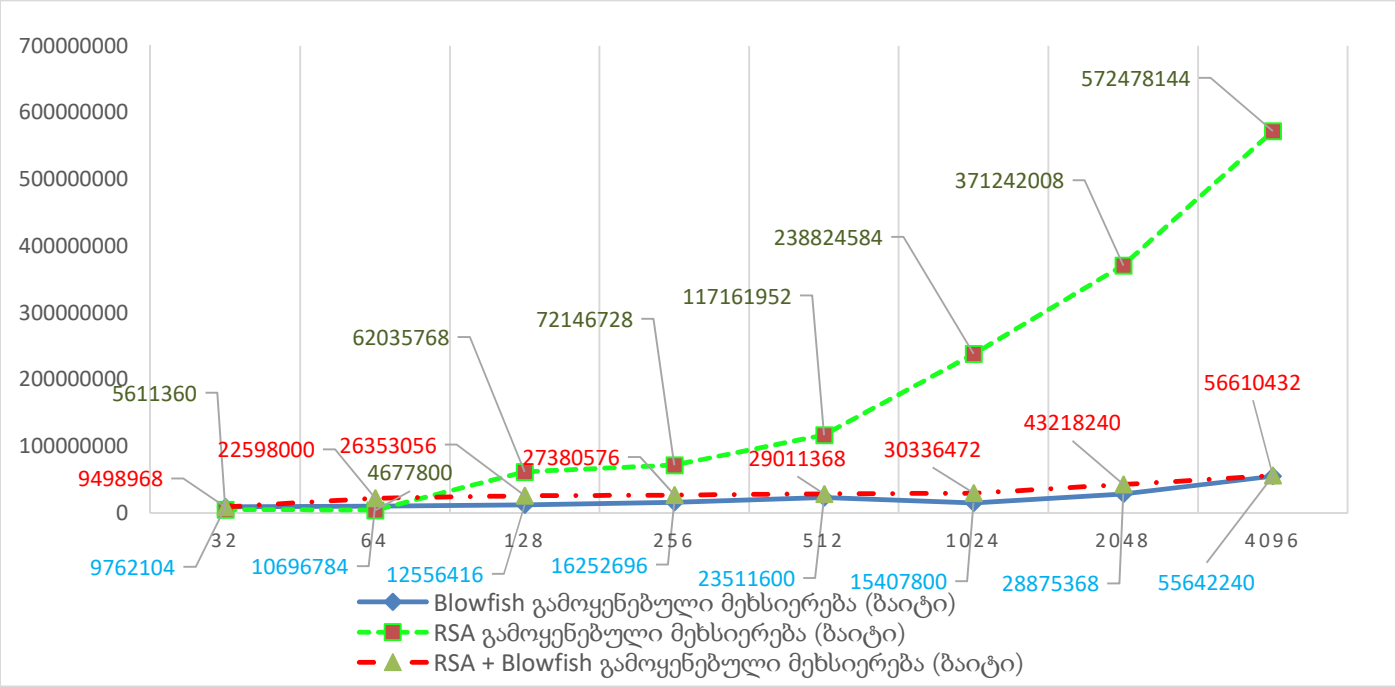
BLOWFISH, AES, IDEA ალგორითმების შედარებისას დგინდება, რომ BLOWFISH მოიხმარს უფრო ნაკლებ ტექნიკურ რესურსს. თუმცა IDEA მოიხმარს ნაკლებ რესურს ვიდრე AES, მაგრამ ჩამორჩება BLOWFISH ალგორითმს.



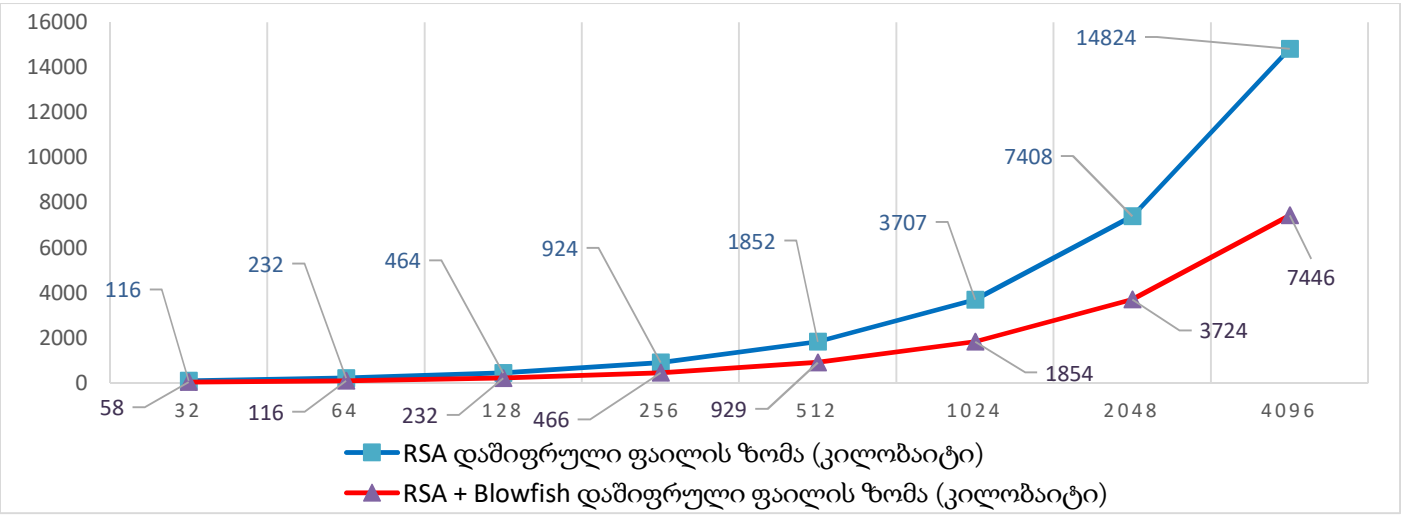

*სურათი 4. Blowfish და RSA + Blowfish კრიპტოსისტემების შიფრაციის პროცესის დროის ვიზუალიზაცია*



***სურათი 5.*** *Blowfish და RSA + Blowfish კრიპტოსისტემების დეშიფრაციის პროცესის დროის ვიზუალიზაცია*




***სურათი 6.*** *Blowfish, RSA და Blowfish+RSA სისტემებში მონაცემების (ბაიტი) შიფრაციისას გამოყენებული მეხსიერების გრაფიკი*




***სურათი 7.*** *RSA და Blowfish+RSA სისტემებში შიფრაციის დროს დაშიფრული ფაილის ზომის ცვლილება*

## დასკვნა

მოცემულ ნაშრომში განხილულია ორი სხვადასხვა სისტემის: სიმეტრიული Blowfish და ასიმეტრიული RSA ალგორითმის პროგრამული რეალიზაცია Java პროგრამირების ენაზე. წარმოდგენილია მოცემული ორი ალგორითმის კომბინაციით მიღებული ჰიბრიდული ალგორითმი და ასევე მისი პროგრამული რეალიზაცია.

მოცემულ ალგორითმებზე ჩატარდა ექსპერიმენტები, რაც ითვალისწინებდა სხვადასხვა ზომის საწყისი მონაცემის დეშიფრაცია/დეშიფრაციის პროცესების შესრულებას სამივე ალგორითმზე. შედეგად ძირითადი დაკვირვების ობიექტს წარმოადგენდა მათი შესრულების დრო და მოხმარებული მეხსიერების მაჩვენებელი. როგორც ჩატარებული ექსპერიმენტები უჩვენებს განხილული ჰიბრიდული ალგორითმი არის უფრო სწრაფი და ამავდროულად უსაფრთხო რადგან გათვალისწინებულია, როგორც სიმეტრიული ასევე ასიმეტრიული ალგორითმის ძლიერი მხარეები.

ჩატარებულმა ექსპერიმენტმა აჩვენა შემდეგი:

1) თუ Blowfish , RSA და Blowfish + RSA ჰიბრიდულ ალგორითმს შევადარებთ **გამოყენებული მეხსიერების მიხედვით** ყველაზე მაღალ ტექნიკურ რესურსს მოითხოვს RSA ალგრითმი, ხოლო Blowfish უმნიშვნელოდ ჩამორჩება Blowfish + RSA ჰიბრიდულ სქემას.
2) **შიფრაციის დროის** პარამეტრის გათვალისწინებით რა თქმა უნდა Blowfish რჩება თავის საწყის პირველ პოზიციაზე და ამ სისტემებში ყველაზე სწრაფია, თუმცა Blowfish + RSA ჰიბრიდული ალგორითმი არც თუ ისე დიდი მნიშვნელობით ჩამორჩება და მნიშვნელოვნად სწრაფია ვიდრე RSA, ხოლო RSA ყველაზე დიდ დროს ანდომებს შიფრაციას და ძალიან ნელია.
3) **დეშიფრაციის დროის** პარამეტრზე დაკვირვებამ აჩვენა, რომ Blowfish + RSA ჰიბრიდული ალგორითმი და Blowfish ალგორითმი თითქმის თანაბარი სისწრაფით ასრულებენ დეშიფრაციის პროცესს და არიან სწრაფი ვიდრე RSA ალგორითმი.
4) **დაშიფრული ფაილის ზომის პარამეტრზე** დაკვირვების შედეგად დადგინდა, რომ ყველაზე დაბალი მეხსიერება სჭირდება Blowfish სისტემას, შემდეგი არის Blowfish + RSA, ხოლო RSA ალგორითმი ყველაზე მაღალი მაცვენებლით ზრდის დაშიფრული ფაილის ზომას.

სამომავლოდ შესაძლებელია განხილული იქნას სხვა სიმეტრიული და ასიმეტრიული ალგორითმის ჰიბრიდული მოდელი, რომლებზეც განხორციელდება ენტროპიული კვლევა, რაც საშუალებას მოგვცემს დავადგინოთ თითოეული მათგანის მდგრადობა სხვადასხვა ტიპის თავდასხმის, მათ შორის დაშიფრული ტექსტის სიხშირული ანალიზის თავდასხმის მიმართ.

## ლიტერატურა


[1] Johhanes A. Buhman, Introduction to Cryptography, Second Edition, 2000

[2] Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanston, Handbook of Applied Cryptography, Massachusetts Institute of Technology, June 1996

[3] Ilya KIZHVATOV, Physical Security of Cryptographic Algorithm Implementations, , L'UNIVERSITÉ DU LUXEMBOURG, 2009

[4] Simson Garfinkel, Alan Schwartz, Gene Spafford, Practical UNIX and Internet Security, 3rd Edition Securing Solaris, Mac OS X, Linux & Free BSD

[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] Phillip Rogaway and Mihir Bellare, Introduction to Modern Cryptography, 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

[17] https://www.techopedia.com/definition/1779/hybrid-encryption

[18] Криптология – наука о тайнописи //Компьютерное обозрение. –1999.

[19] Мао В. Современная криптография: Теория и практика — М.: Вильямс, 2005

[20] Ященко В. В. Введение в криптографию. СПб.: Питер, 2001.

[21] Hamdan O. Alanazi, B. B. Zaidan, A. A. Zaidan, Hamid A. Jalab, M. Shabbir and Y. Al-Nabhani, "New Comparative Study Between DES, 3DES and AES within Nine factors", Journal of Computing, Volume, 2, Issue 3, March 2010, pp. 152-157.

[22] Dr. Prerna Mahajan and Abhishek Sachdeva, " A study of Encryption Algorithms AES, DES and RSA for Security", Global Journal of Computer Science and Technology Network, Web & Security, Volume 13 Issue 15 Version 1.0 Year 2013, pp. 15-22.

[23] Deepak Kumar Dakate and Pawan Dubey, "Performance comparison of Symmetric Data Encryption Techniques", International Journal of Advanced Research in Computer Engineering and Technology, Volume 3, No. 8, August 2012, pp. 163-166.

[24] Abdel-Karim Al Tamimi, "Performance Analysis of Data Encryption Algorithms."

[25] Sumitra, "Comparative Analysis of AES and DES security Algorithms", International Journal of Scientific and Research Publications, Volume 3, Issue 1, January 2013, pp. 1-5.

[26] Ayushi, 2010,A Symmetric Key Cryptographic Algorithm, International Journal of Computer Applications (0975 - 8887) Volume 1. No. 15, 2010

[27] "Quantum cryptography: An emerging technology in network security". - Sharbaf, M.S. IEEE International Conference on Technologies for Homeland Security . 2011

[28] The official Advanced Encryption Standard" (PDF). Computer Security Resource Center. National Institute of Standards and Technology. Retrieved 26 March 2015.

[29] "The Digital Millennium Copyright Act of 1998" (PDF). United States Copyright Office. Retrieved 26 March 2015.

[30] Cramer, Ronald; Shoup, Victor (2004). "Design and Analysis of Practical Public-Key Encryption Schemes Secure against Adaptive Chosen Ciphertext Attack"

[31] Hofheinz, Dennis; Kiltz, Eike (2007). "Secure Hybrid Encryption from Weakened Key Encapsulation". Advances in Cryptology -- CRYPTO 2007