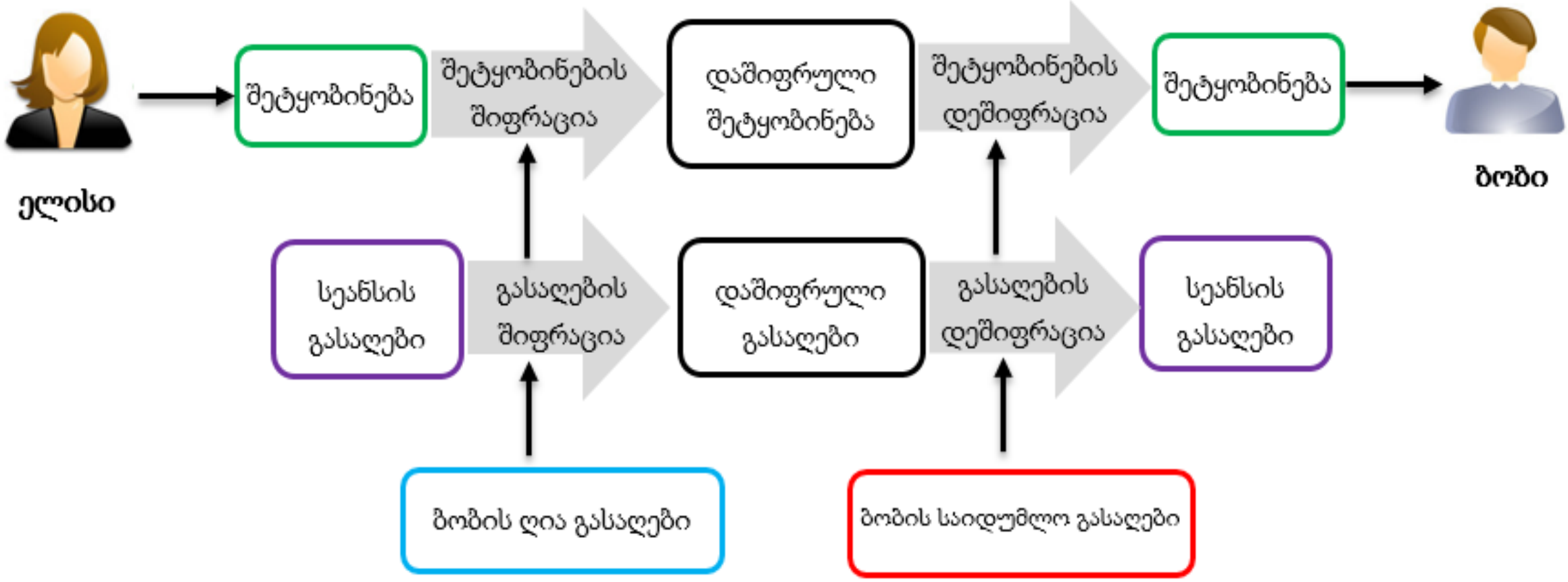
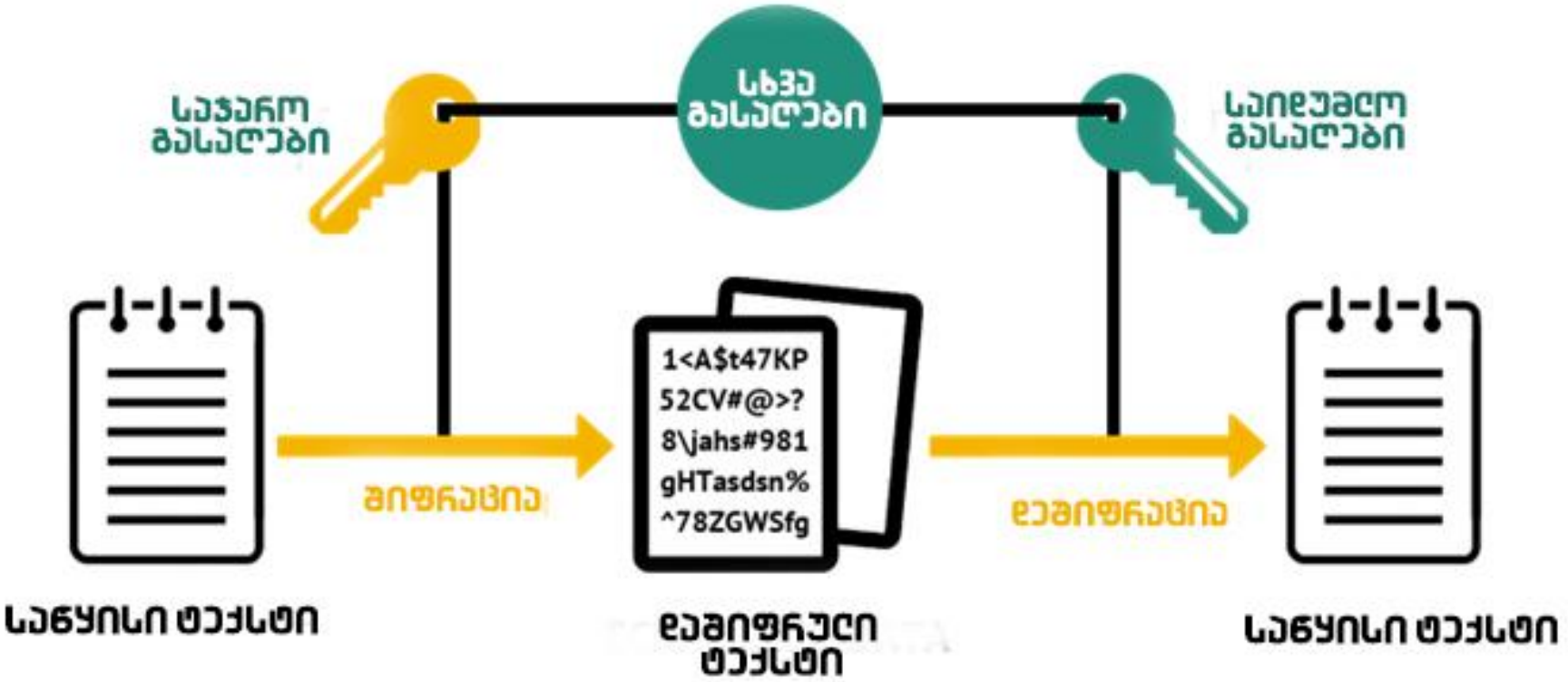
თანამედროვე ჰიბრიდული კრიპტოსისტემები

ელზა ჯინჭარაძე

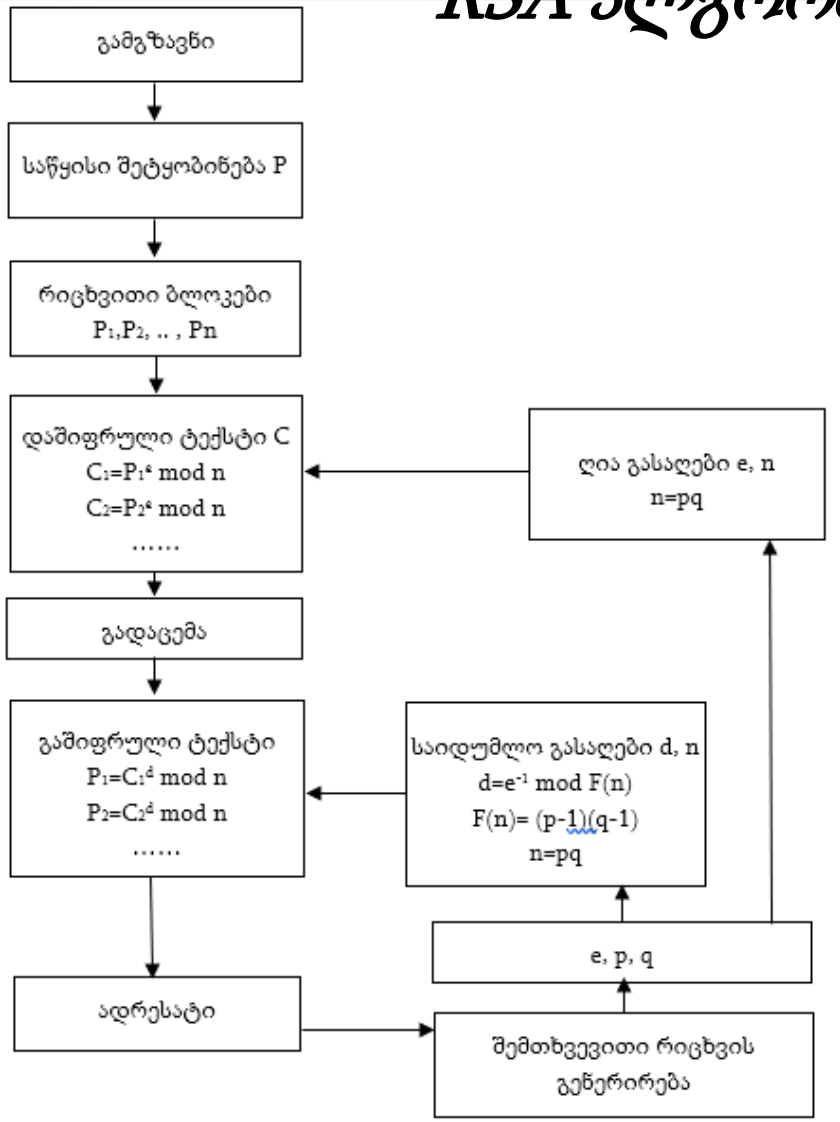
ჰიბრიდული კრიპტოსისტემის ზოგადი სქემა



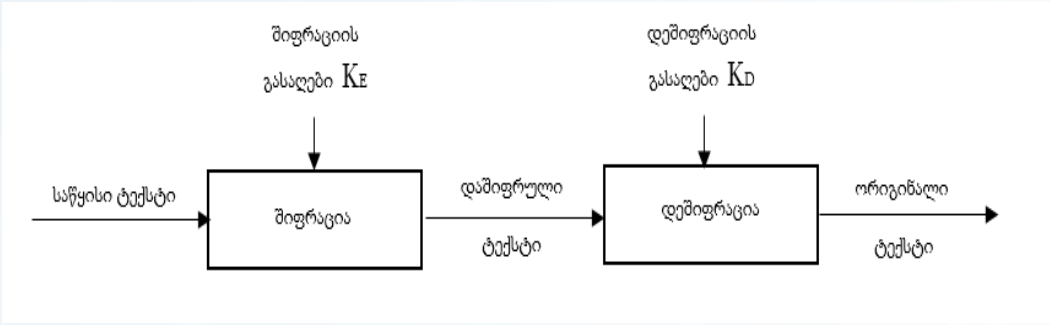
ასიმეტრიული შიფრაცია



RSA ალგორითმის სტრუქტურა



ასიმეტრიული კრიპტოგრაფიული ალგორითმის ზოგადი სქემა, $K_E \neq K_D$



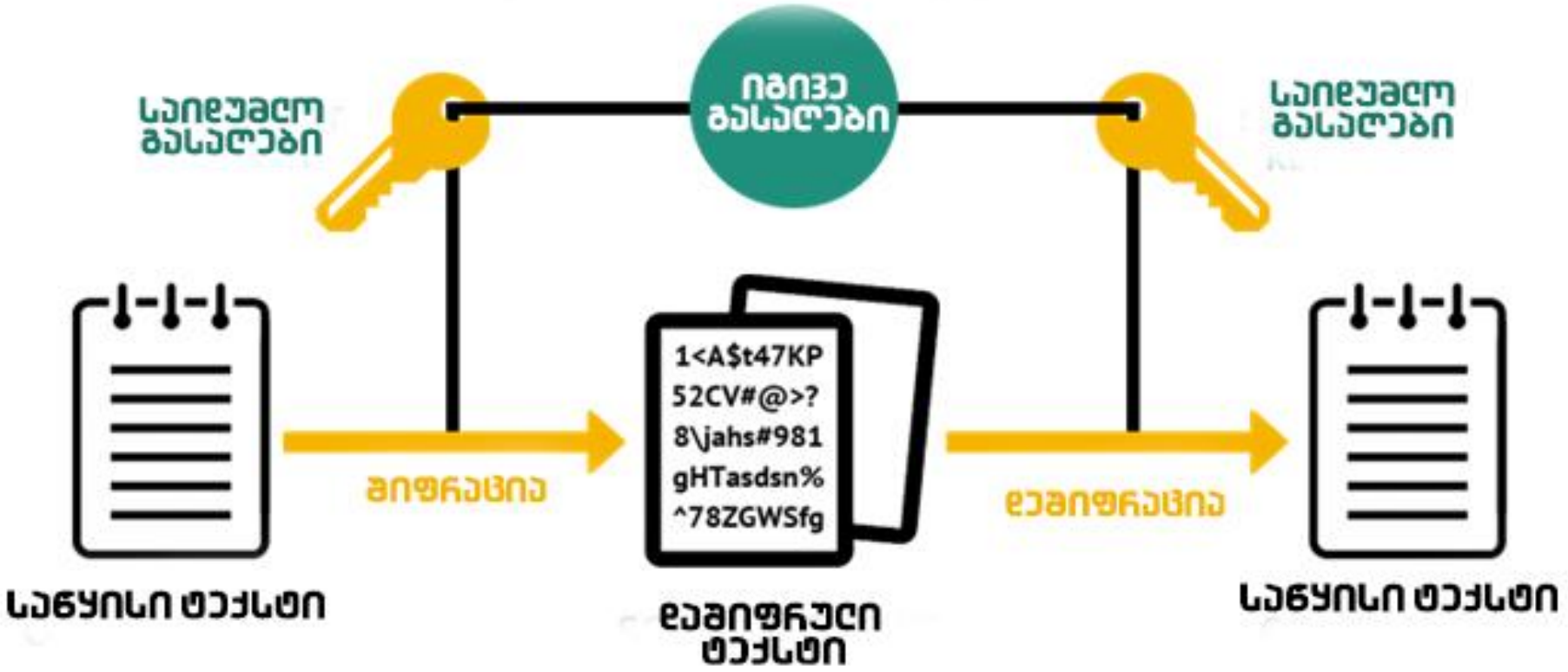
უპირატესობა:

- უსაფრთხოება
- აუთენტიფიკაცია

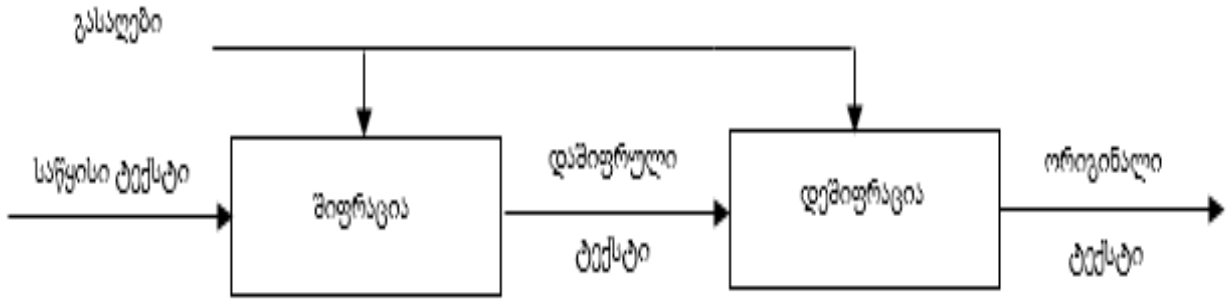
ნაკლოვანება:

- სირთულე

სიმეტრიული შიფრაცია



Blowfish ალგორითმის სტრუქტურა



$E_K(M)=C$

$D_K(C)=M$

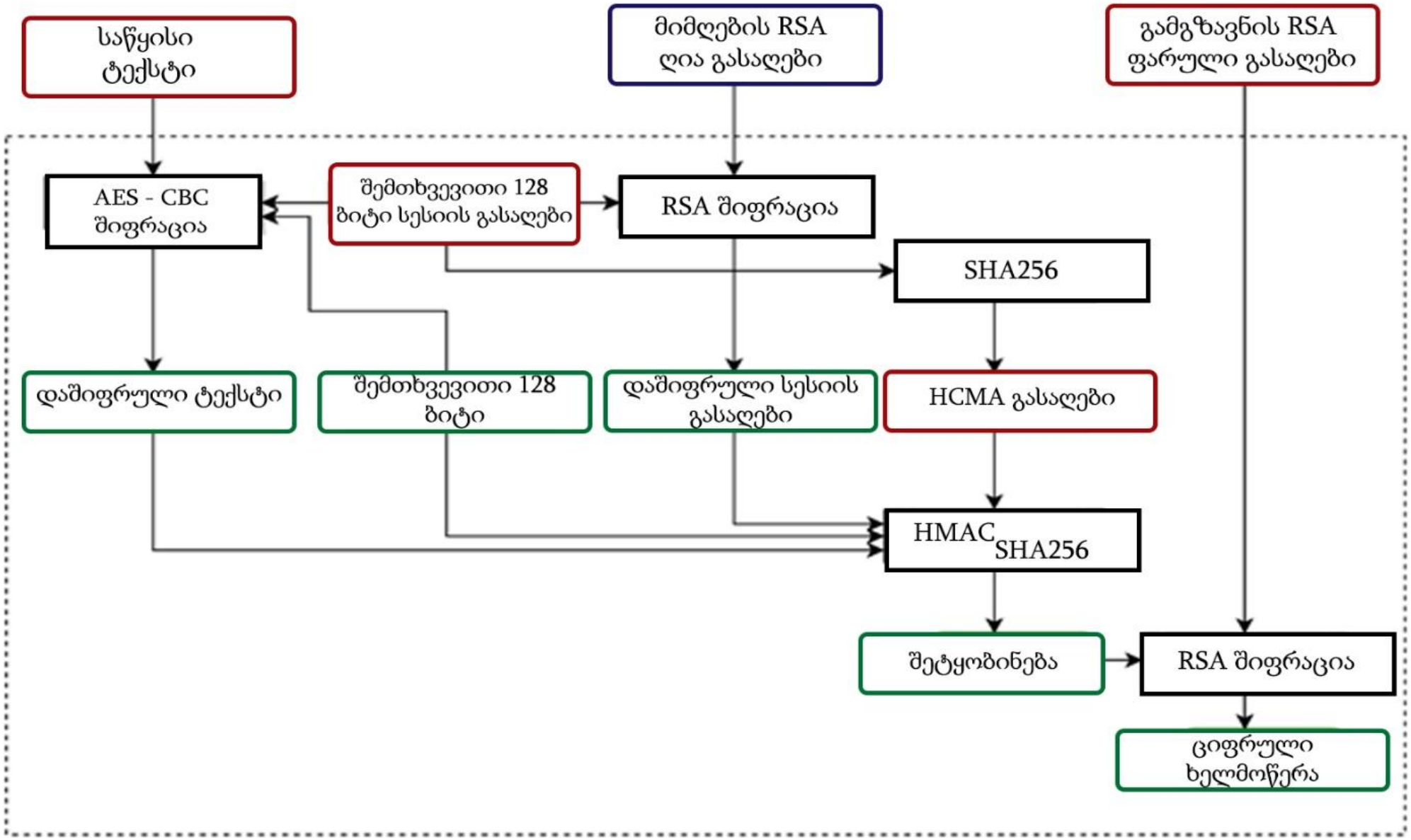
$M=D_K(E_K(M))$

უპირატესობა:

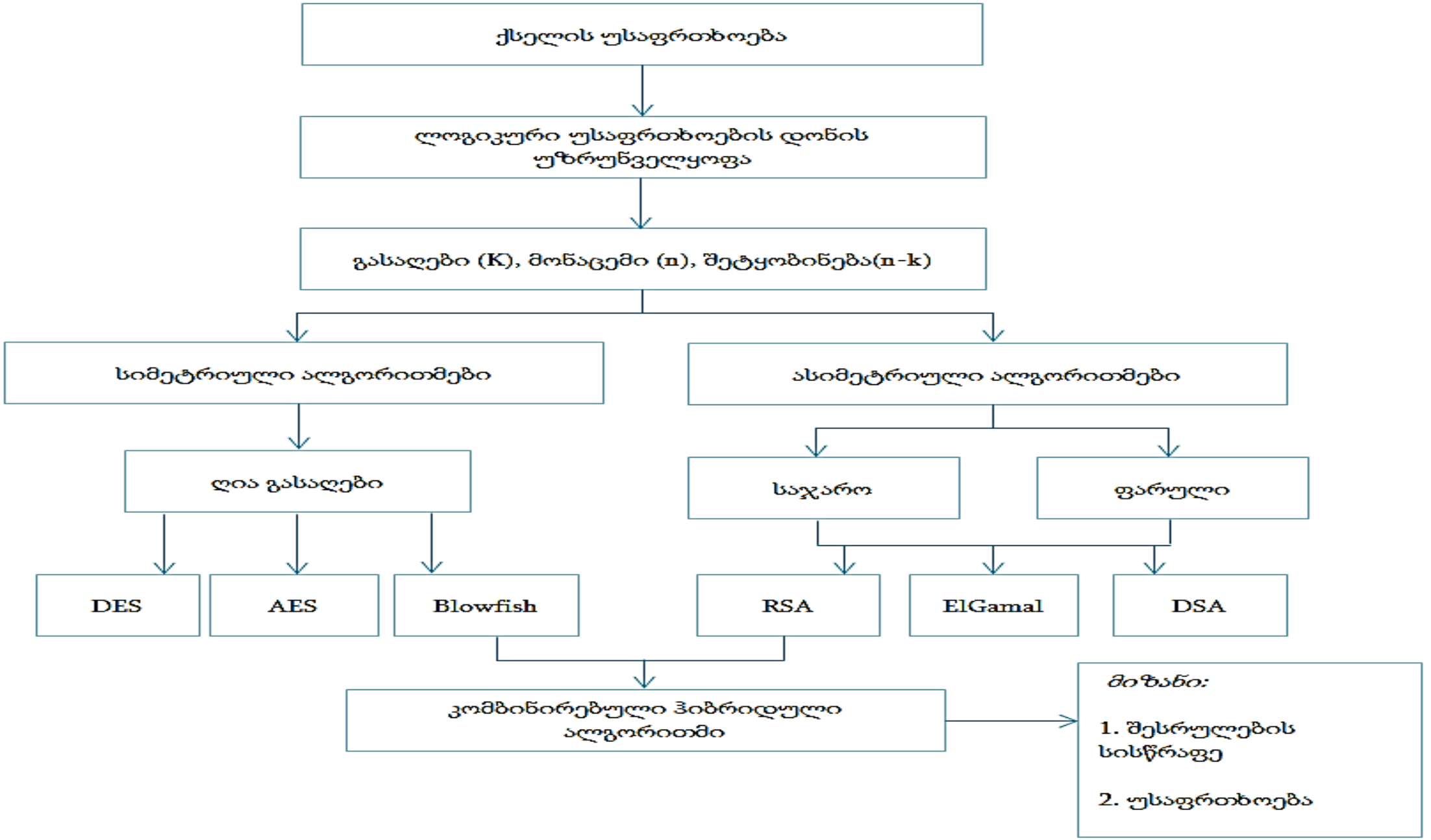
- სიმარტივე
- სისწრაფე

ნაკლოვანება:

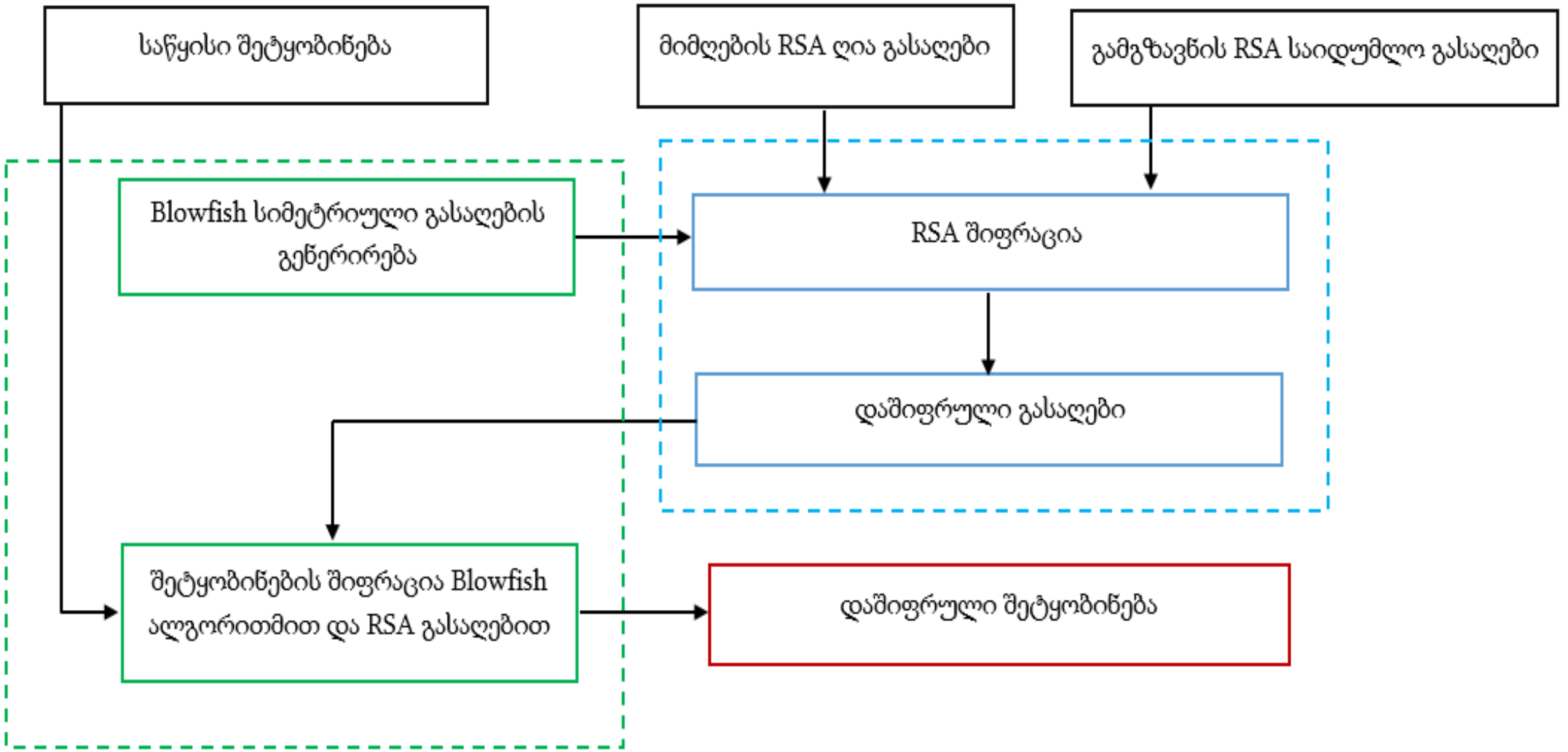
- ნაკლებად უსაფრთხო



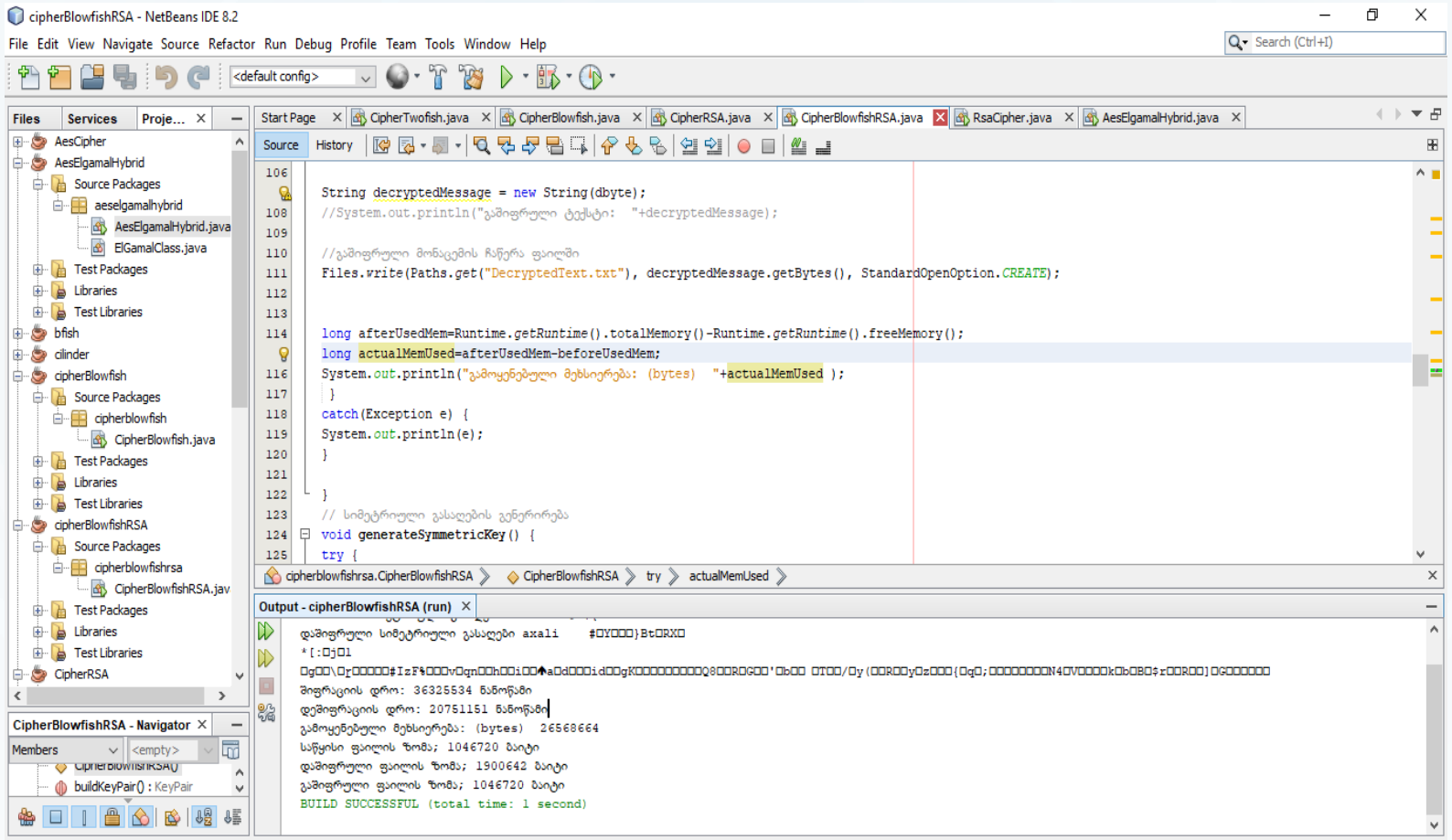
ჰიბრიდული სქემის მოდელი



ჰიბრიდული კრიპტოსისტემის ზოგადი სქემა



RSA + Blowfish კრიპტოსისტემების კომბინაციით მიღებული ჰიბრიდული კრიპოსისტემის ზოგადი არქიტექტურა



პროგრამული კოდის შესრულება (ფრაგმენტი)

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

Blowfish დეშიფრაცია

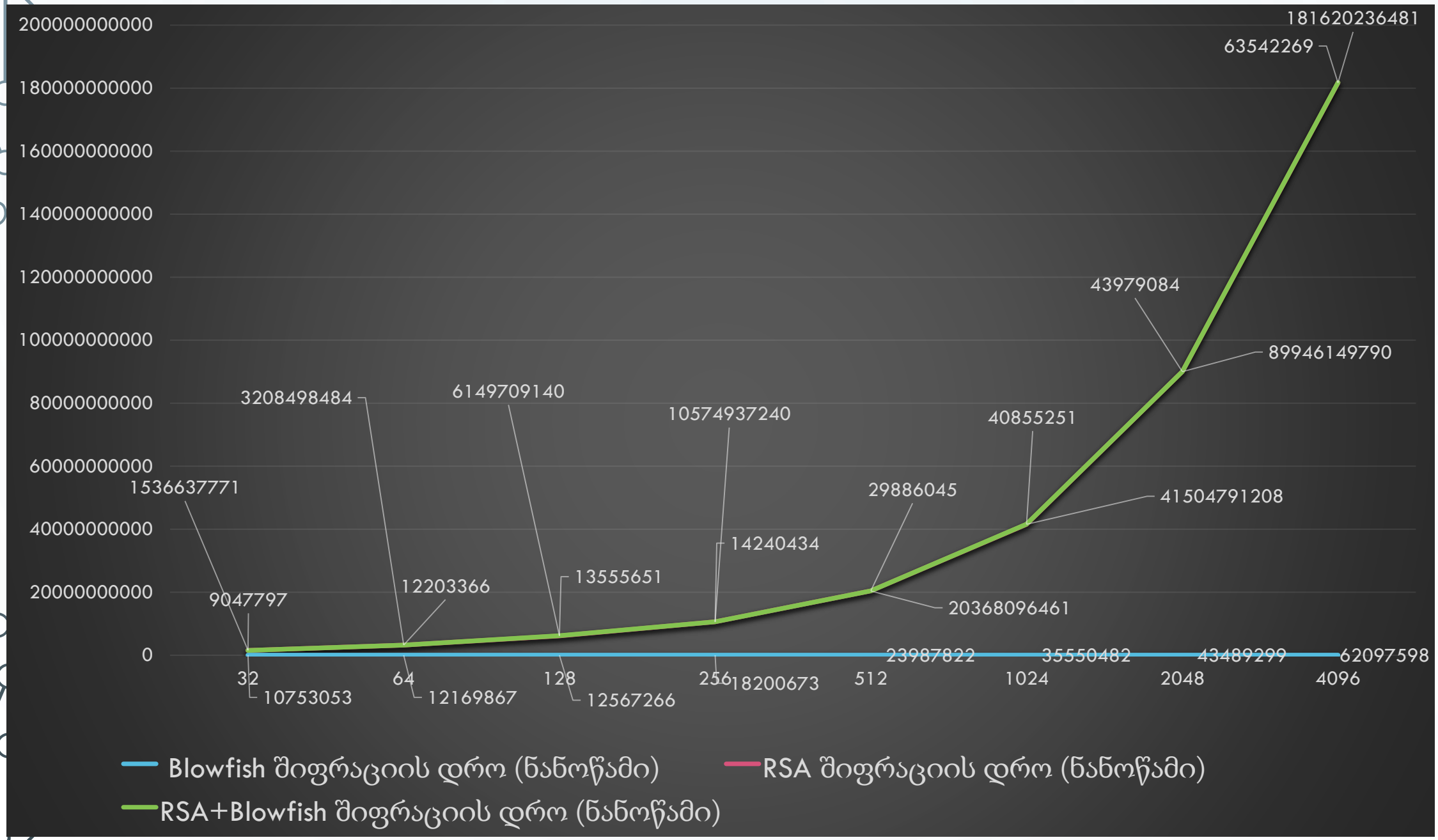
დასაშიფრი ტექსტის ზომა (კილობაიტი)	დასაშიფრი ტექსტის ზომა (ბაიტი)	გასაღების ზომა (ბიტი)	დეშიფრაციის დრო (ნანოწამი)	დაშიფრული ტექსტის ზომა (ბაიტი)
58	59241	16	1984528	32710
117	119493	16	2743007	65420
231	236670	16	5602025	130840
465	475738	16	9356337	261680
932	954280	16	16802548	523360
1871	1915678	16	26062972	1048460
3715	3804367	16	40463494	2096920
7375	7552059	16	56950097	4193840

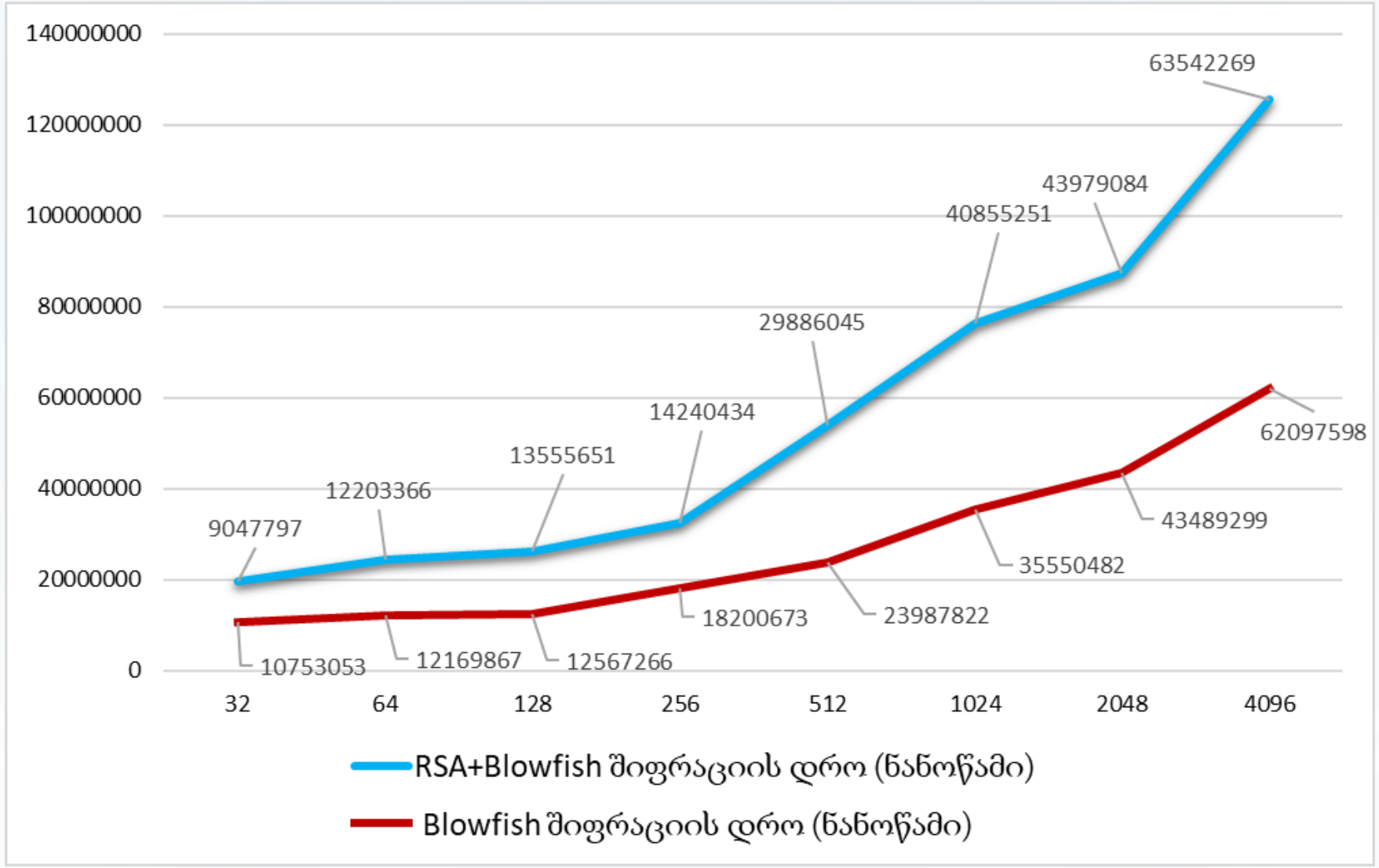
RSA შიფრაცია			
ფაილის ზომა (KB)	საწყისი ფაილის ზომა (Byte)	შიფრაციის დრო (ნანოწამი)	დაშიფრული ტექსტის ზომა
32	32710	1536637771	118780
64	65420	3208498484	237689
128	130840	6149709140	474654
256	261680	10574937240	946614
512	523360	20368096461	1896331
1024	1048460	41504791208	3795983
2048	2096920	89946149790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

RSA დეშიფრაცია			
ფაილის ზომა (KB)	საწყისი ფაილის ზომა (Byte)	დეშიფრაციის დრო (ნანოწამი)	დაშიფრული ტექსტის ზომა
116	118780	55542452	32710
232	237689	121344997	65420
464	474654	284935252	130840
924	946614	671696785	261680
1852	1896331	1991097468	523360
3707	3795983	6934459468	1048460
7408	7586016	27974097086	2096920
14824	15179673	121238321204	4193840

Blowfish + RSA შიფრაცია			
ფაილის ზომა (KB)	საწყისი ფაილის ზომა (Byte)	შიფრაციის დრო (ნანოწამი)	დაშიფრული ტექსტის ზომა
32	32710	9047797	59355
64	65420	12203366	118428
128	130840	13555651	237417
256	261680	14240434	477370
512	523360	29886045	951418
1024	1048460	40855251	1898922
2048	2096920	43979084	3813804
4096	4193840	63542269	7624638

Blowfish + RSA ჰიბრიდული კრიპტოსისტემის შიფრაციის პროცესი

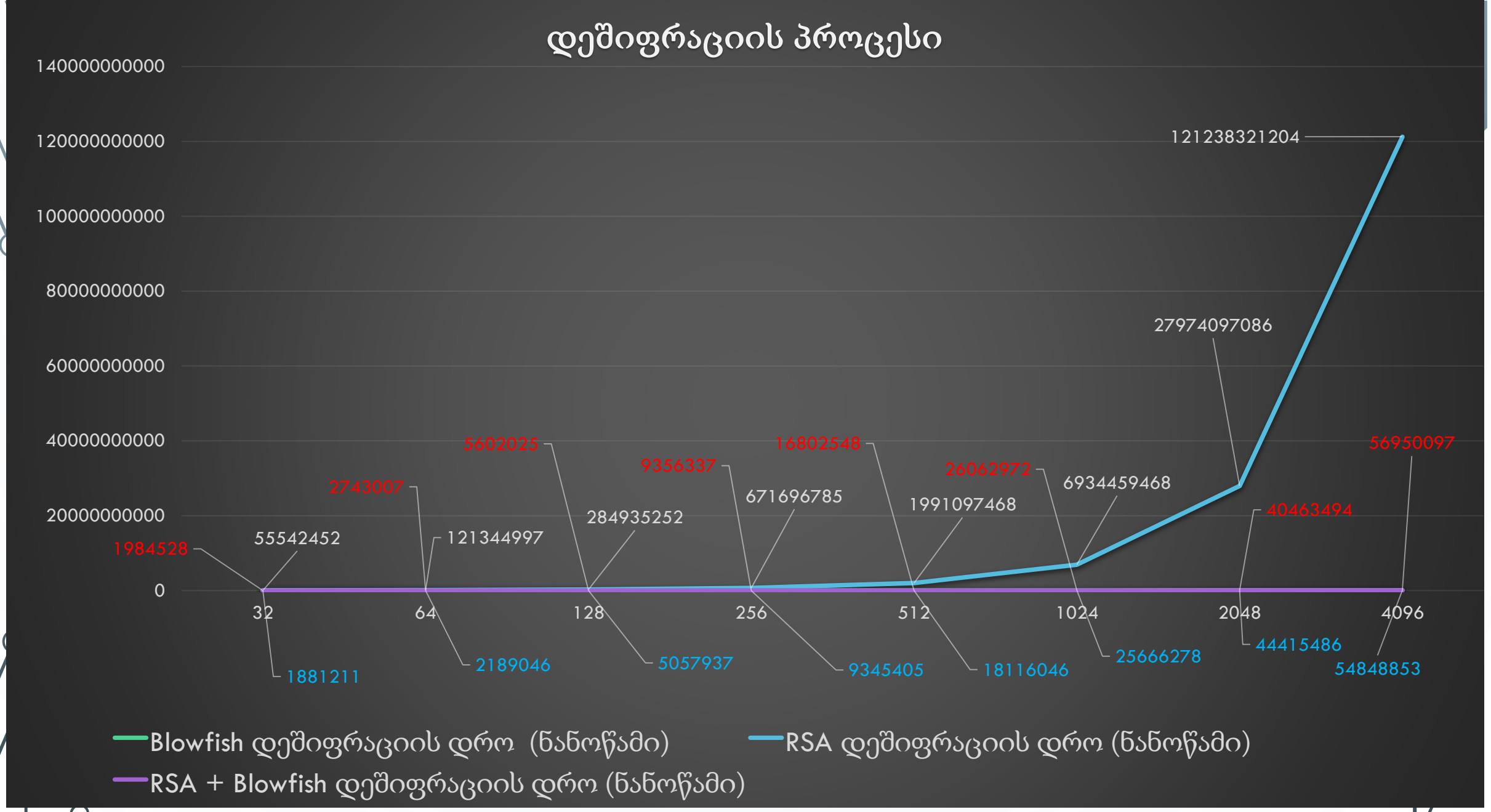

200000000000
180000000000
160000000000
140000000000
120000000000
100000000000
80000000000
60000000000
40000000000
20000000000
0
1536637771
9047797
3208498484
12203366
6149709140
13555651
10574937240
14240434
29886045
20368096461
40855251
41504791208
43979084
89946149790
181620236481
63542269
32
10753053
64
12169867
128
12567266
256
18200673
512
23987822
1024
35550482
2048
43489299
4096
62097598
Blowfish შიფრაციის დრო (ნანოწამი)
RSA შიფრაციის დრო (ნანოწამი)
RSA+Blowfish შიფრაციის დრო (ნანოწამი)

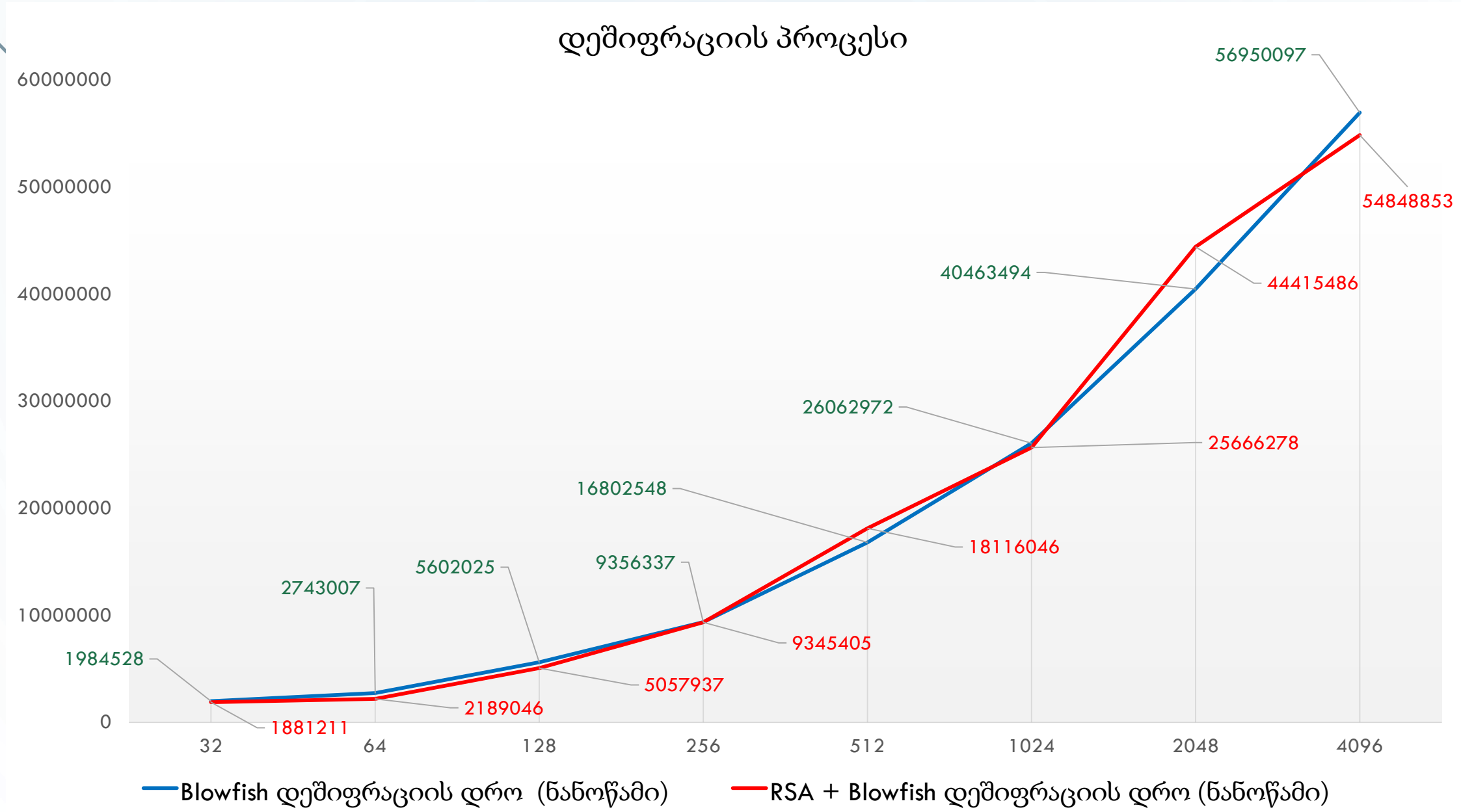


Blowfish და RSA + Blowfish კრიპტოსისტემების შიფრაციის პროცესის დროის ვიზუალიზაცია

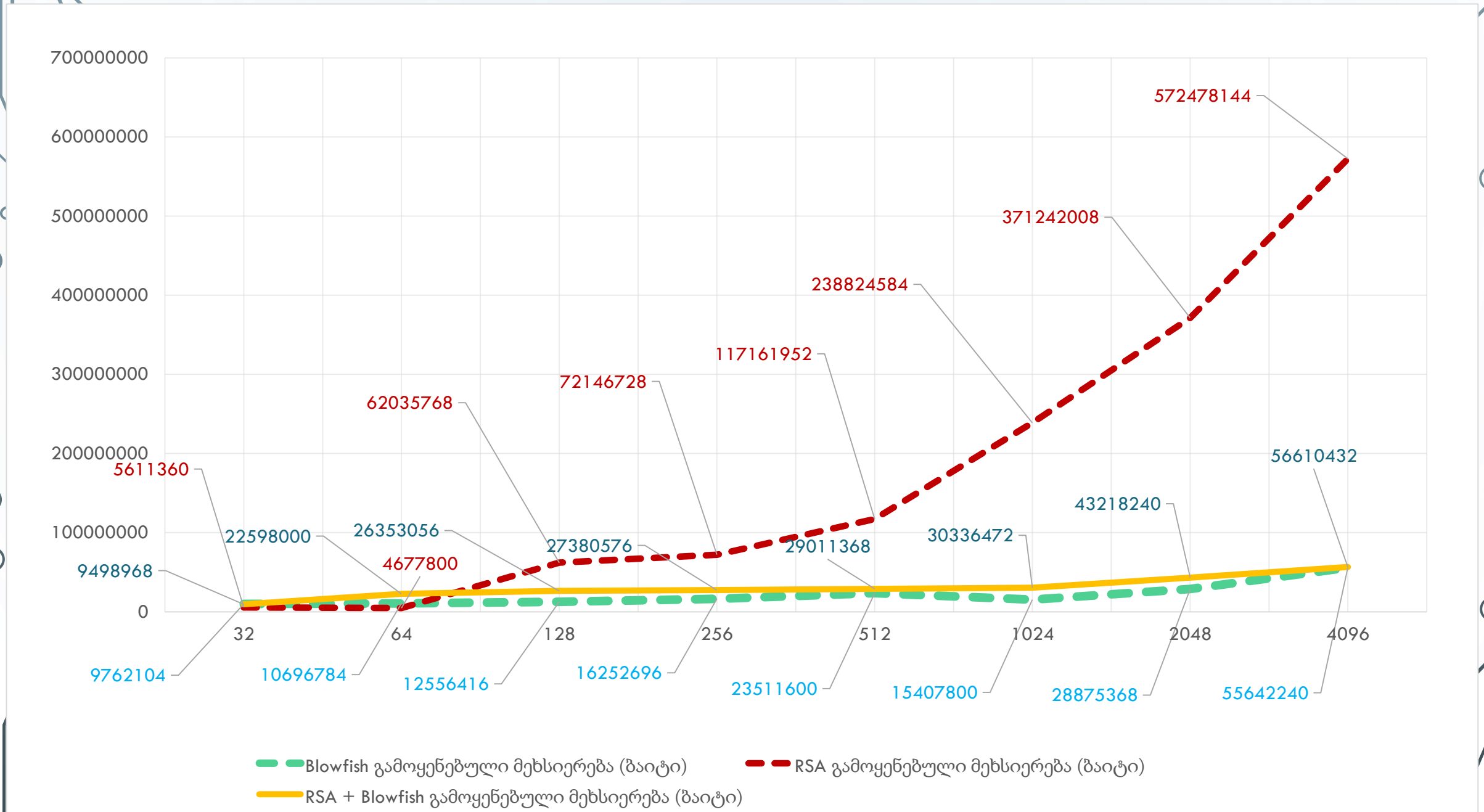
Blowfish + RSA დეშიფრაცია			
ფაილის ზომა (KB)	საწყისი ფაილის ზომა (Byte)	დეშიფრაციის დრო (ნანოწამი)	დაშიფრული ტექსტის ზომა (ბაიტი)
58	59355	1881211	32710
116	118428	2189046	65420
232	237417	5057937	130840
466	477370	9345405	261680
929	951418	18116046	523360
1854	1898922	25666278	1048460
3724	3813804	54415486	2096920
7446	7624638	54848853	4193840

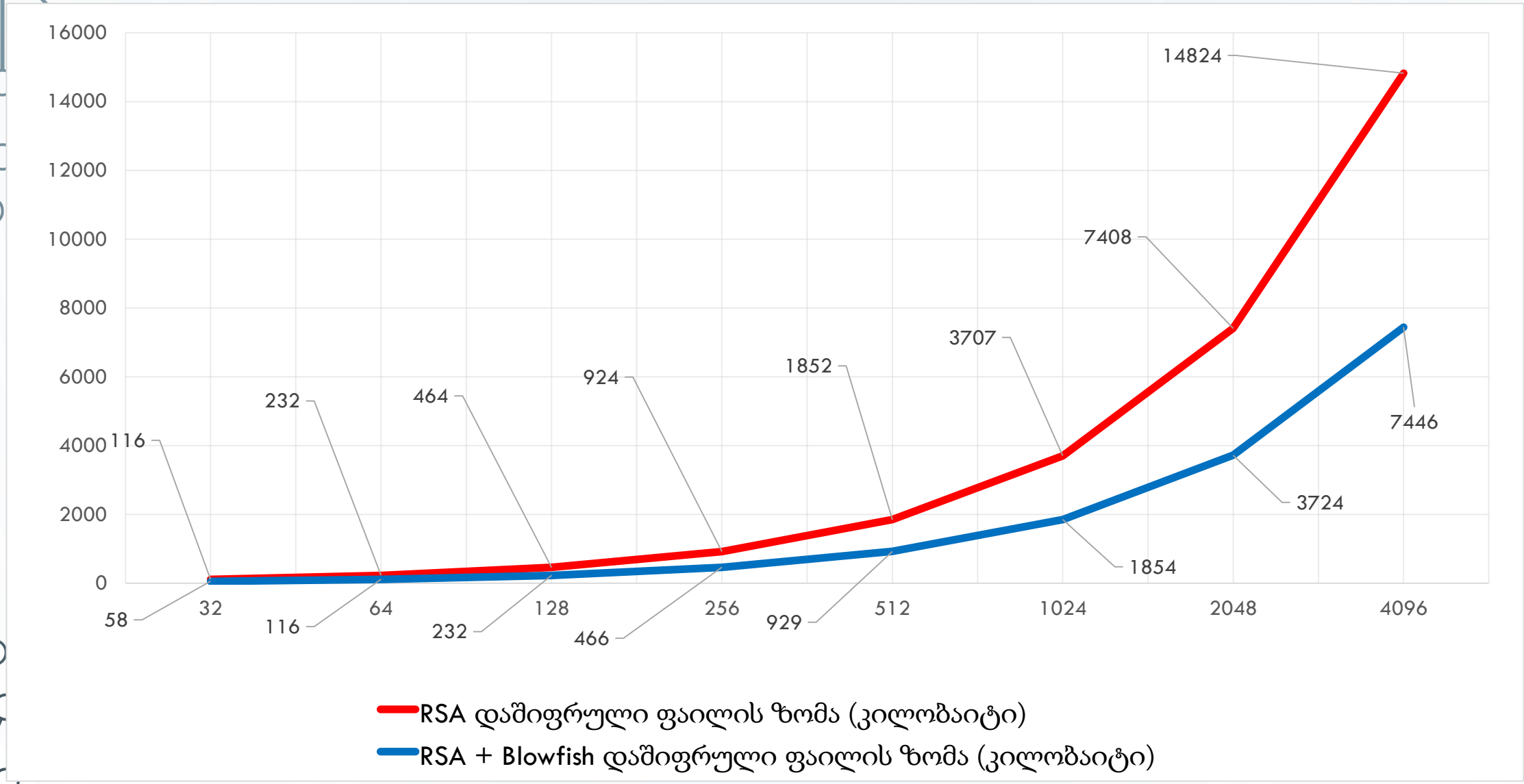
Blowfish + RSA ჰიბრიდული კრიპტოსისტემის დეშიფრაციის პროცესი


დეშიფრაციის პროცესი
140000000000
120000000000
100000000000
80000000000
60000000000
40000000000
20000000000
0
32
64
128
256
512
1024
2048
4096
1984528
55542452
2743007
121344997
5602025
284935252
9356337
671696785
16802548
1991097468
26062972
6934459468
27974097086
121238321204
40463494
56950097
1881211
2189046
5057937
9345405
18116046
25666278
44415486
54848853
Blowfish დეშიფრაციის დრო (ნანოწამი)
RSA დეშიფრაციის დრო (ნანოწამი)
RSA + Blowfish დეშიფრაციის დრო (ნანოწამი)



Blowfish და RSA + Blowfish კრიპტოსისტემების დეშიფრაციის პროცესის დროის ვიზუალიზაცია


700000000
600000000
500000000
400000000
300000000
200000000
100000000
0
32
64
128
256
512
1024
2048
4096
5611360
62035768
72146728
117161952
238824584
371242008
572478144
9498968
22598000
26353056
27380576
29011368
30336472
43218240
56610432
9762104
4677800
10696784
12556416
16252696
23511600
15407800
28875368
55642240
Blowfish გამოყენებული მეხსიერება (ბაიტი)
RSA გამოყენებული მეხსიერება (ბაიტი)
RSA + Blowfish გამოყენებული მეხსიერება (ბაიტი)

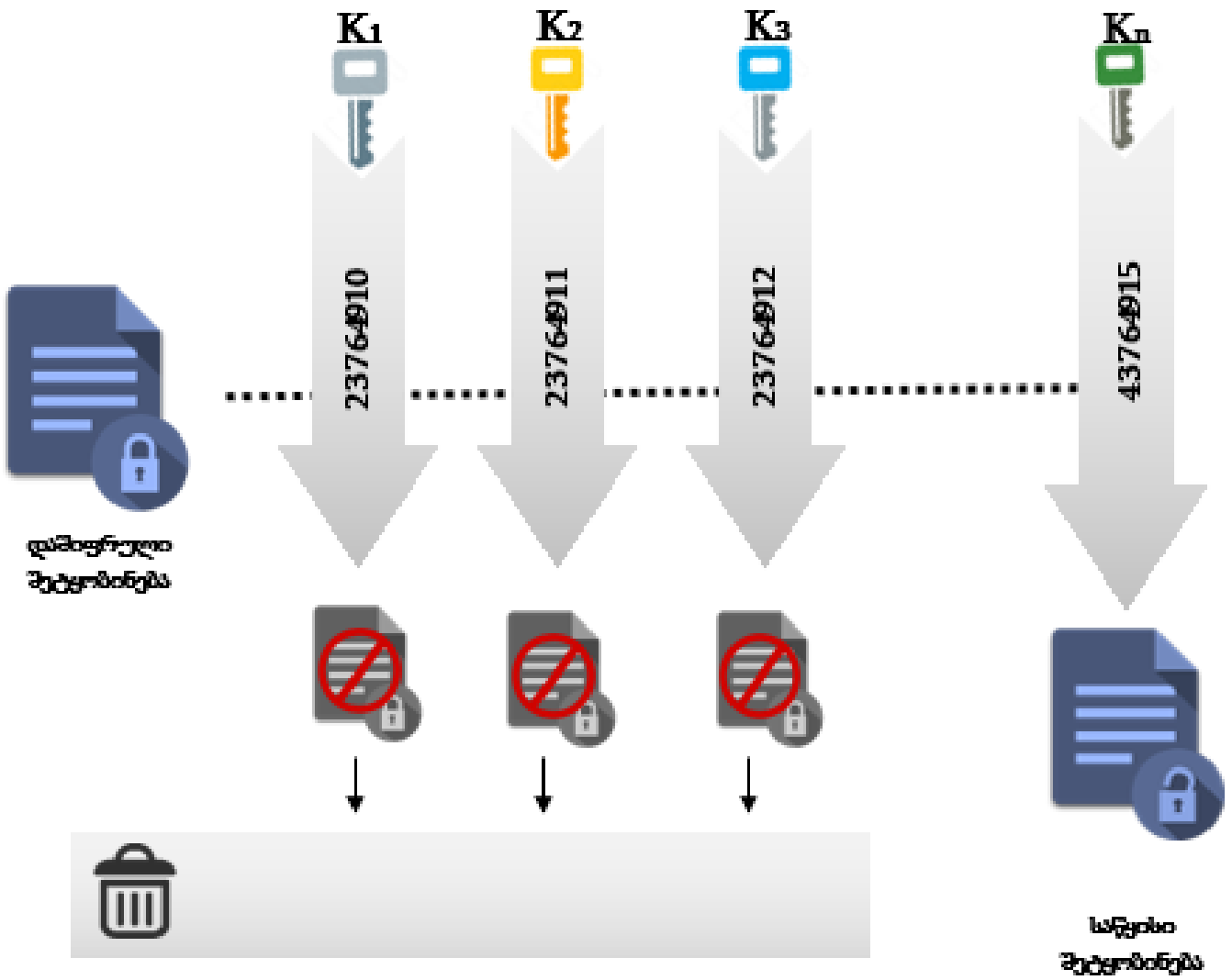


RSA და Blowfish+RSA სისტემებში შიფრაციის დროს დაშიფრული ფაილის ზომის ცვლილება

სიმეტრიული ალგორითმების მოკლე მიმოხილვა და ზოგადი დახასიათება

ალგორითმი	აღწერა	გასაღების სიგრძე	რეიტინგი
Blowfish	ბლოკური ალგორითმი	1-448 ბიტი	ითვლება ძლიერ ალგორითმად, თუმცა მნიშვნელოვნად ჩამორჩება სხვა გაცილებით ძლიერ და სწრაფ ალგორითმებს.
DES	1977 აღიარებული იქნა ა.შ.შ მიერ	56 ბიტი	მოკლე გასაღებისა და მათემატიკური სისუსტის გამო ამ ალგორითმის გამოყენება აღარ არის რეკომენდირებული.
IDEA	ბლოკური ალგორითმი	128 ბიტი	ითვლება ძლიერ ალგორითმად, თუმცა მნიშვნელოვნად ჩამორჩება სხვა უფრო ძლიერ და სწრაფ ალგორითმებს.
RC2	ბლოკური ალგორითმი	1-2048 ბიტი	საუკეთესო ალგორითმი. ეს ალგორითმი ფართოდ გამოიყენება, იყენებს გასაღებთა რაოდენობის საკმარისი სიგრძის რაოდენობას.
RC4	ნაკადური ალგორითმი	1-2048 ბიტი	ითვლება ძლიერ ალგორითმად, თუმცა მნიშვნელოვნად ჩამორჩება სხვა უფრო ძლიერ და სწრაფ ალგორითმებს. მოკლე გასაღებისა და მათემატიკური სისუსტის გამო ამ ალგორითმის გამოყენება აღარ არის რეკომენდირებული.
AES (Rijndael)	შექმნილია Daemen და Rijmen მიერ	128-256 ბიტი	საუკეთესო ალგორითმი. ეს ალგორითმი ფართოდ გამოიყენება, იყენებს გასაღებთა რაოდენობის საკმარისი სიგრძის რაოდენობას.

თავდასხმა უხეში ძალის მეთოდით (brute force)



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

გასაღების სიგრძე	1 წამში მოძიებული გასაღების რაოდენობა	გასაღების ძიების დროს გამოყენებული ტექნიკური რესურსი	ყველა გასაღების ძიების სავარაუდო დრო
40 ბიტი	1,000	ჩვეულებრივი დესკტოპ კომპიუტერი	35 წელი
40 ბიტი	1 მილიონი	დესკტოპ კომპიუტერების პატარა ქსელი	13 დღე
56 ბიტი	1 მილიარდი	საშუალო ზომის კორპორატიული ქსელი	2.5 წელი
56 ბიტი	100 მილიარდი	ტექნოლოგია DES ალგორითმის დეშიფრაციისთვის	8 დღე
64 ბიტი	1 მილიარდი	საშუალო ზომის კორპორატიული ქსელი	585 წელი
80 ბიტი	1 მილიარდი	დესკტოპ კომპიუტერების პატარა ქსელი	38 მილიარდი წელი
80 ბიტი	1 მილიარდი	საშუალო ზომის კორპორატიული ქსელი	38 მილიონი წელი
128 ბიტი	1 მილიარდი	საშუალო ზომის კორპორატიული ქსელი	10^{22} წელი
192 ბიტი	1 x 10^{23}	სპეციალური დანიშნულების კვანტური კომპიუტერი 2015 წლის მონაცემებით	2 x 10^{27} წელი
256 ბიტი	1 x 10^{23}	სპეციალური დანიშნულების კვანტური კომპიუტერი 2015 წლის მონაცემებით	3.7 x 10^{46} წელი
256 ბიტი	1 x 10^{32}	სპეციალური დანიშნულების კვანტური კომპიუტერი 2015 წლის მონაცემებით	3.7 x 10^{37} წელი

AES + ElGamal

AES უპირატესობები

- გასაღების სიგრძის ზრდასთან ერთად იზრდება უსაფრთხოება; 128, 192, 256
- 128 ბიტიანი გასაღების გატეხვა მოითხოვს 2^{128} ოპერაციას
- ყველაზე პოპულარული ელ. კომერციაში, ელ.ბიზნესში, ფინანსურ ტრანზაქციებში

AES ნაკლოვანებები

- მარტივი მათემატიკური სტრუქტურა
- ყველა ბლოკი ერთნაირად იშიფრება
- რთულია პროგრამული ინტეგრაცია, პროგრამული სისწრაფისა და უსაფრთხოების ერთდროულად შენარჩუნება

ElGamal უპირატესობები

- გვაქვს რამდენიმე გასაღები
- შიფრაციის ყოველ ეტაპზე გვაქვს სხვადასხვა შიფრაციის გასაღები
- იყენებს დიდ რიცხვთა არითმეტიკას. (BigInteger)

ElGamal ნაკლოვანებები

- დაშიფრული ტექსტი მნიშვნელოვნად აღემატება საწყის ტექსტს
- მოითხოვს შიფრაციის დიდ დროს

ElGamal კრიპტოსისტემა

ეტაპი N1 - გასაღების გენერირება;

- შემთხვევითი მარტივი p რიცხვის გენერირება ;
- g გენერატორი, $g < p$;
- მთელი x რიცხვის არჩევა, $1 < x < p$;
- ხდება $y = g^x \ mod \ p$ გამოსახულების გამოთვლა;
- y, g და p ღია გასაღებები
- x ფარული გასაღები

ეტაპი N2 - საწყისი შეტყობინების შიფრაცია;

- M შეტყობინება. მთელი k გასაღების არჩევა. $1 < k < p - 1$;
- 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.

ეტაპი N3 - დაშიფრული შეტყობინების დეშიფრაცია.

$$M = b \ (a^x)^{-1} \ mod \ p$$

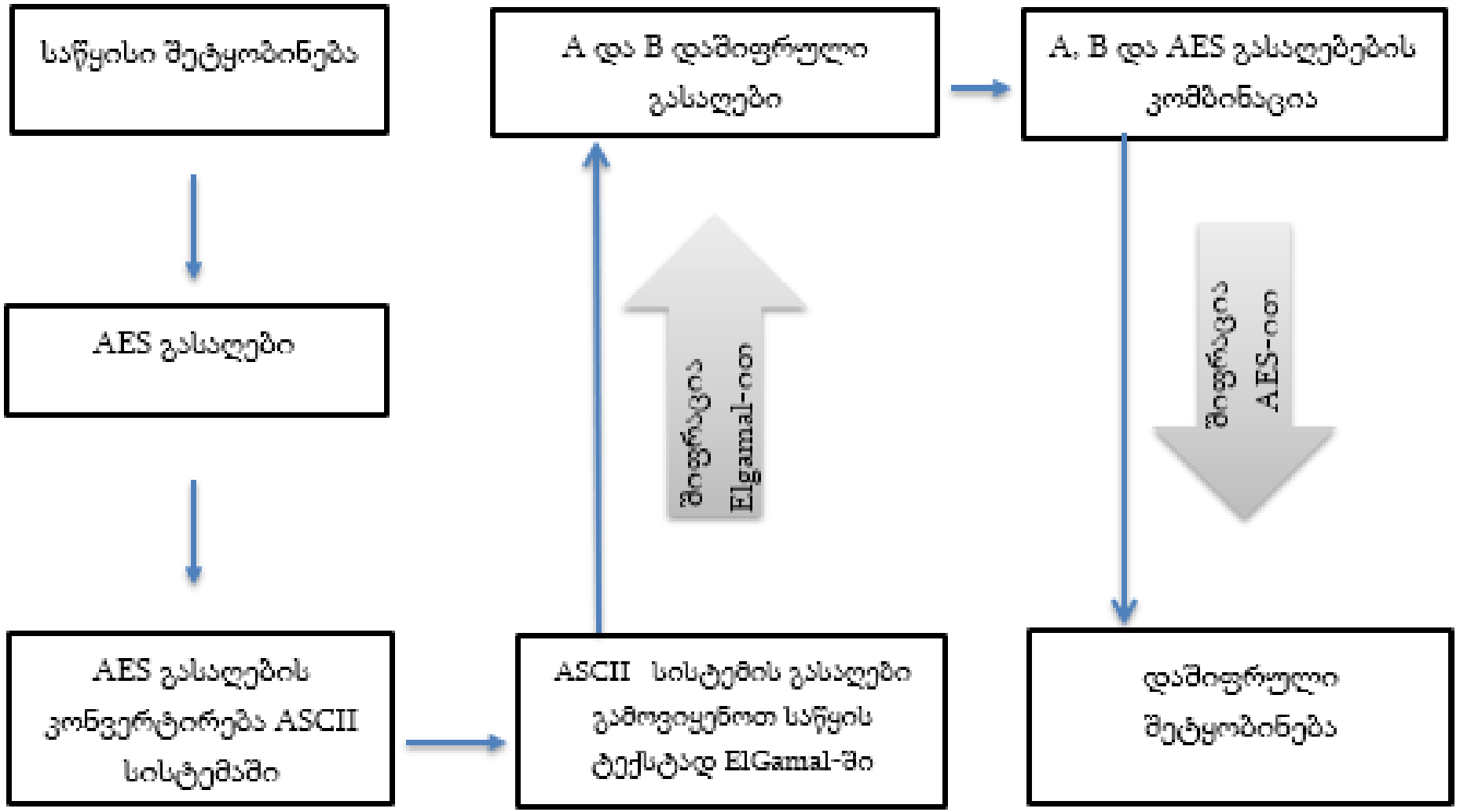
ოპერაციული სისტემა	**Windows 10**
პროცესორი	Intel Core i7-7500U up to 3.5 Ghz
ოპერატიული მეხსიერება	8GB DDR4
ვიდეო დაფა	Nvidia GeForce 940MX 2GB

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

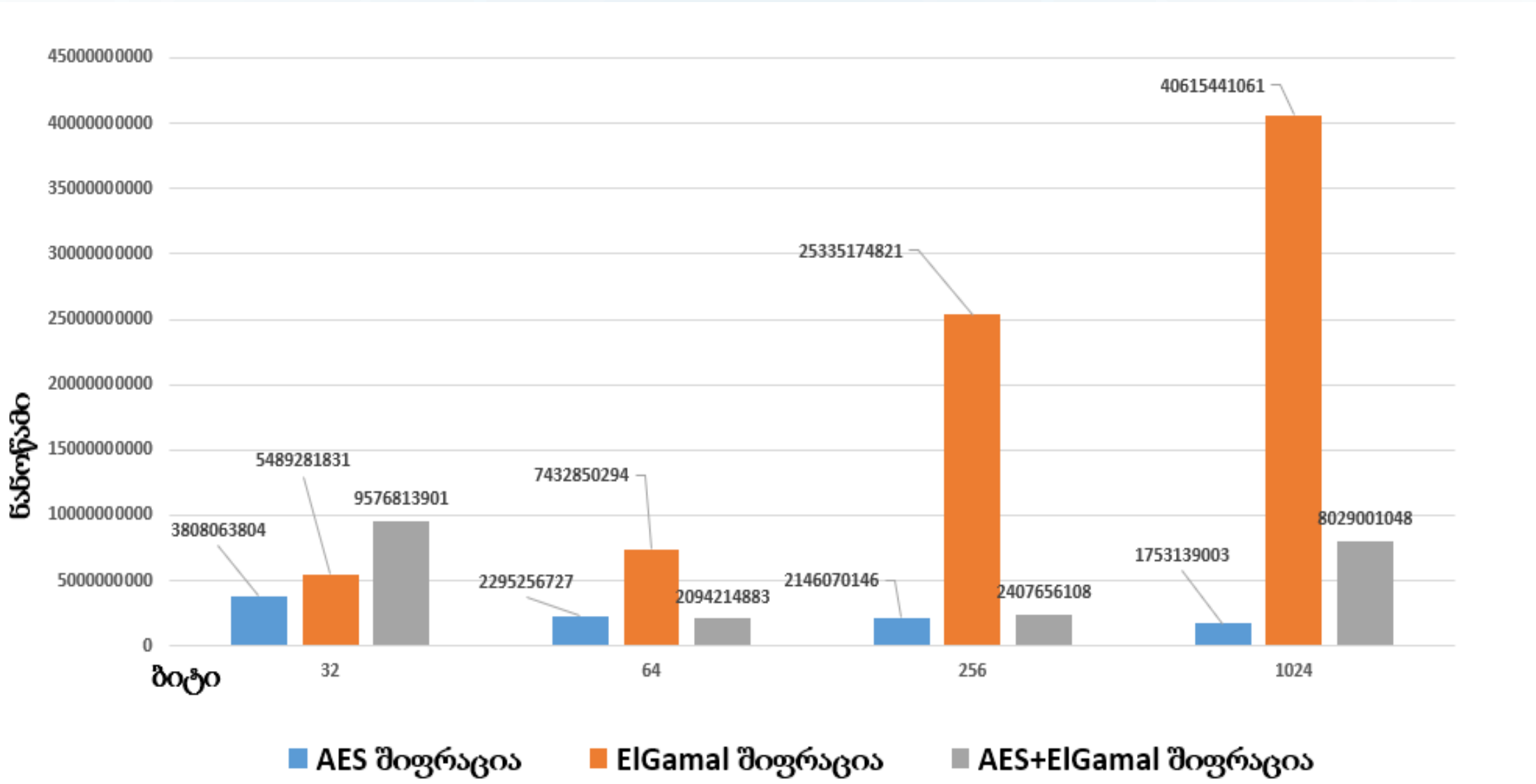
ElGamal შიფრაცია		
მონაცემის ზომა	დრო	გამოყენებული მეხსიერება
32 ბიტი	5489281831 ნანოწამი	4027936 ბიტი
64 ბიტი	7432850294 ნანოწამი	4027096 ბიტი
512 ბიტი	25335174821 ნანოწამი	7388952 ბიტი
1024 ბიტი	40615441061 ნანოწამი	11409872 ბიტი
ElGamal დეშიფრაცია		
32 ბიტი	1403419 ნანოწამი	4027936 ბიტი
64 ბიტი	2290604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

AES + ElGamal კრიპტოსისტემების კომბინაციით მიღებული ჰიბრიდული კრიპოსისტემის ზოგადი არქიტექტურა



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

საწყისი მონაცემების (ბიტი) შიფრაციისა და დროის (ნანოწამი) დამოკიდებულების გრაფიკი



მადლობა ყურადღებისთვის!