UDC 513.21
SCOPUS CODE 1700
https://doi.org/10.36073/1512-0996-2025-1-392-400

სიმეტრიული და ასიმეტრიული შიფრაციის გამოყენება კიბერუსაფრთხოებაში

ნოდარ ლომინაძე საინფორმაციო ტექნოლოგიების დეპარტამენტი, საქართველოს ტექნიკური უნივერსიტეტი, საქართველო, 0160, თბილისი, მ. კოსტავას 69
E-mail: n.lominadze@gtu.ge

თამარ ლომინაძე საინფორმაციო ტექნოლოგიების დეპარტამენტი, საქართველოს ტექნიკური უნივერსიტეტი, საქართველო, 0160, თბილისი, მ. კოსტავას 69
E-mail: t.lominadze@gtu.ge

თამარ ასათიანი საინფორმაციო ტექნოლოგიების დეპარტამენტი, საქართველოს ტექნიკური უნივერსიტეტი, საქართველო, 0160, თბილისი, მ. კოსტავას 69
E-mail: t.asatiani@gtu.ge

რეცენზენტები:

რ. კაკუბავა, სტუ-ის ინფორმატიკისა და მართვის სისტემების ფაკულტეტის პროფესორი
E-mail: r.kakubava@gtu.ge

ი. ქართველიშვილი, სტუ-ის ინფორმატიკისა და მართვის სისტემების ფაკულტეტის პროფესორი
E-mail: s.kartvelishvili@gtu.ge

ანოტაცია. ინფორმაციული უსაფრთხოების სისტემების განვითარება და მათი ეფექტურობის გაზრდა განიხილება HTTPS-ის მაგალითზე, რომელიც HTTP პროტოკოლის გაუმჯობესებული ვერსიაა. HTTPS მონაცემთა დაცვას უზრუნველყოფს კომუნიკაციის დროს.

TCP/IP პროტოკოლების გამოყენება ინტერნეტში საიმედო მონაცემთა გადაცემის საფუძველია, თუმცა ვერ უზრუნველყოფს მონაცემთა კონფიდენციალურობას. ამისთვის საჭიროა დამატებითი უსაფრთხოების შრე, როგორიცაა SSL/TLS პროტოკოლი, რომელიც კლიენტსა და სერვერს შორის უსაფრთხო კავშირებს უზრუნველყოფს. SSL/TLS პროტოკოლები ერთ-ერთი მნიშვნელოვანი ტექნოლოგიაა. კლიენტსა და სერვერს შორის მისი გამოყენება, შიფრაციისა და დეშიფრაციის ალგორითმებით, იცავს კავშირს დანაშაულებრივი ჩარევისგან. ეს პროცესი მათემატიკურ მოდელებს და ალგორითმებს ეფუძნება, რომლებიც მუდმივად საჭიროებს განახლებას, რათა შეძლოს უპასუხოს კიბერუსაფრთხოების თანამედროვე გამოწვევებს.

განხილულია კომპიუტერში კლიენტ-სერვერული ურთიერთობის მახასიათებლების ეფექტუროე-

ბის მაჩვენებლის გაუმჯობესების საკითხები, შიფრების კრებულების რაციონალურად შერჩევის საფუძველზე. აქცენტირებულია ელიპტიკურ წირზე დაფუძნებული კრიპტოგრაფიის გამოყენების საკითხები, როგორიცაა ECDHE (ელიპტიკურ წირზე დაფუძნებული დიფ-ჰელმანის ეფემერული ალგორითმი) და ECDSA (ელიპტიკურ წირზე დაფუძნებული ციფრული ხელმოწერის ალგორითმი), რაც საშუალებას იძლევა, შემცირდეს გამოყენებული შიფრთა კრებულების რაოდენობა და ამავე დროს კომპიუტერულ ქსელში გაუმჯობესდეს კომუნიკაციის მახასიათებლები.

საკვანძო სიტყვები: Eliptic curve Cryptography, ECC; Elliptic Curve Diffie – Hellman Ephemeral ECDHE; Elliptic Curve Digital Singonture Algorithm ECDSA; HTTP Sequre; TLS.

შესავალი

მიუხედავად იმისა, რომ კიბერუსაფრთხოების სფეროში მიღწეულია გარკვეული წარმატებები, დღეისთვის კვლავ არსებობს სხვადასხვა გამოწვევა, რომელთა გადალახვა მასშტაბურ კვლევებსა და საინჟინრო სამუშაოებს მოითხოვს. აღნიშნული კვლევების აუცილებლობა გამოწვეულია სიტუაციით, რომელიც შემდეგნაირად შეიძლება აღიწეროს:

1. მათემატიკური მოდელები ინფორმაციული უსაფრთხოების სისტემებში. კიბერუსაფრთხოების სფეროში ერთ-ერთი ძირითადი ასპექტია მათემატიკური მოდელების გამოყენება. ისინი მონაცემთა დაცვის სისტემების დიზაინისა და იმპლემენტაციის ხელსაწყოებია. თუმცა არ გამოირიცხება, რომ დღეს გამოყენებული მოდელებისთის დამუშავდეს ახალი სქემები, რომელთა გამოყენება საერთოდ შეცვლის საიმედოდ მიჩნეულ არსებულ მეთოდებს. ამ პროცესის განხორციელება დიდ რესურსებს და დროს მოითხოვს.

2. კვანტური კომპიუტერის განვითარების პერსპექტივა. არსებობს მოსაზრება, რომ კვანტური კომპიუტერული ტექნოლოგიის გამოყენებით, რთული ალგორითმები შეიძლება გახდეს მარტივი და სწრაფად აღსრულებადი. ამჟამად მიმდინარეობს კვლევა თუ რომელ დონეზე უნდა დაინერგოს კვანტური კომპიუტერები და რომელი ალგორითმები და პარამეტრები შეინარჩუნებს ქმედით მისი არსებობის პირობებში.

3. ახალი პროტოკოლებისა და სტანდარტების შექმნა. კიბერუსაფრთხოების სფეროში ახალი პროტოკოლებისა და სტანდარტების შემუშავება, მათი გავრცელება და დანერგვა ხანგრძლივ დროს მოითხოვს. ეს პროცესი მოიცავს ახალი ალგორითმის მახასიათებლის კვლევებს, რომელიც წლობით მუშაობას გულისმობს. შესაბამისი სტანდარტის შემუშავების (მაგ., NIST) და აღიარების შემდგომ იწყება მისი გავრცელების პროცესი, რომელიც ასევე ხანგრძლივია. შერჩეული და აღიარებული სტანდარტები ხშირად ვრცელდება ნელა, რადგან ზოგიერთი ორგანიზაცია არ ეთანხმება ამ ცვლილებებს და მოსალოდნელია, რომ პარალელურად მოხდეს როგორც ძველი სტანდარტების, ისე ახლის გამოყენება, ხოლო ქსელმა უნდა უზრუნველყოს ორ კვანძს შორის კომუნიკაციის შესაძლებლობა. ეს კვანძებს აიძულებს უზრუნველყოს როგორც არსებული, ისე განახლებული სტანდარტების მუშაობა.

ჰაკერებისა და სხვა ორგანიზაციების გავლენა. ტექნიკური მოწყობილობები, როგორც წესი, მდგრადად მუშაობს სპეციფიკაციის შესაბამისად, თუმცა ხშირად, როდესაც სხვადასხვა ორგანიზაცია და პირი არაკანონიერ მიზნებს ისახავს, ერევა ამ მოწყობილობების მუშაობაში, ვითარება იცვლება. მაგალითად, ჰაკერები მუდმივად ეძებენ უსაფრთხოების ხარვეზებს პროტოკოლებში, რათა არამართებული გზით გამოიყენონ ისინი, ხოლო ზოგიერთი ორგანიზაცია აყენებს მოთხოვნას პროგრამისტების წინაშე, რათა მათი სისტემები შეიცავდეს ე.წ. "უკანა შესასვლელებს", რომლებიც საშუალებას მისცემს დიდი მოცულობის მონაცემებიდან კონკრეტული ინფორმაცია ადვილად ამოიღონ.

ძირითადი ნაწილი

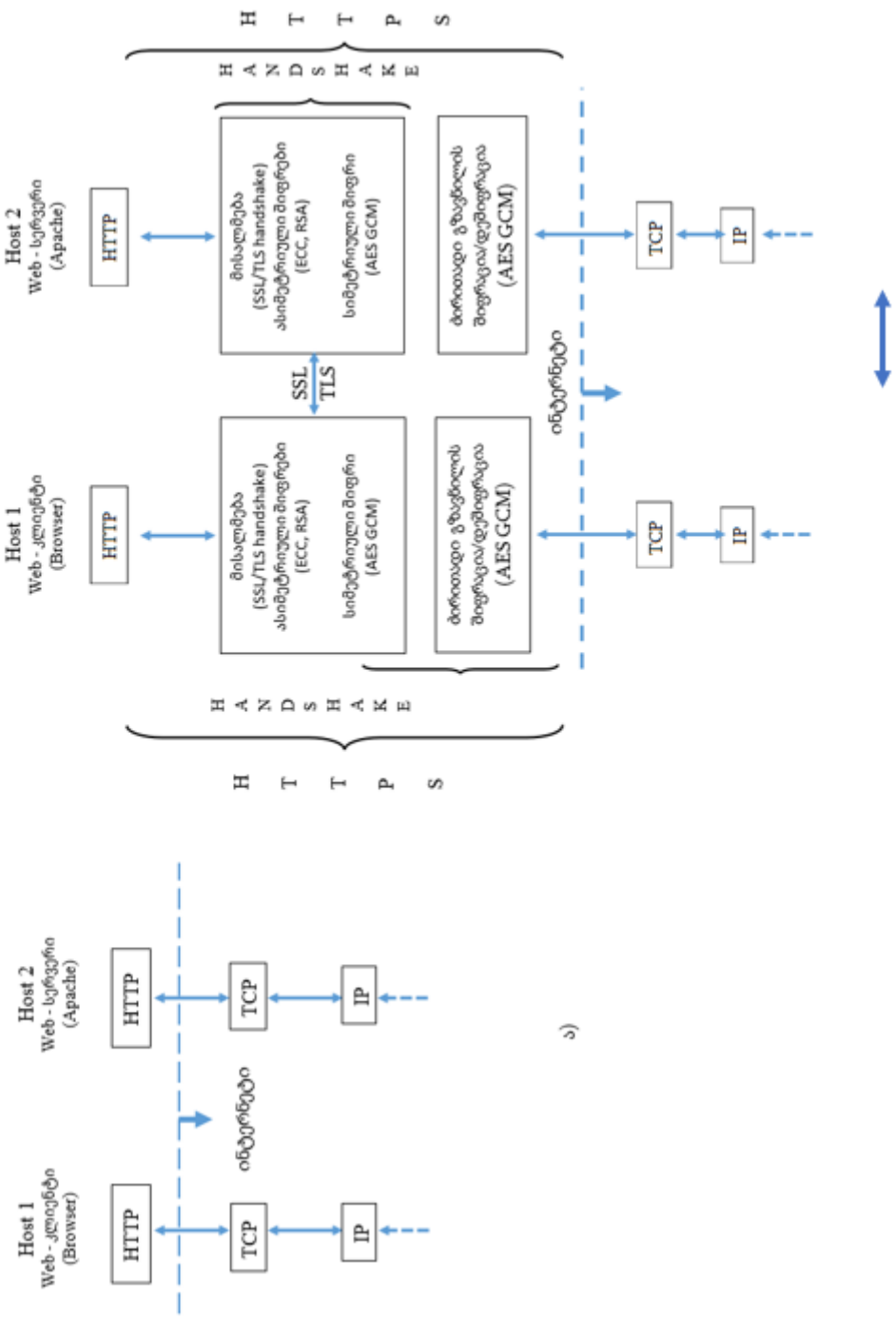
ტრანსპორტის დონის უსაფრთხოება

განვიხილოთ ინფორმაციული უსაფრთხოების განვითარების ძირითადი ეტაპები და პერსპექტივები HTTPS გამოყენებითი სისტემის მაგალითზე, რომელიც HTTP პროტოკოლის გაუმჯობესებული ვერსიაა, (HTTP Sequre). მისი ფუნქციონირების ზოგადი სქემა ნაჩვენებია 1-ელ სურათზე.

როგორც 1-ელი სურათი გვიჩვენებს, გამოყენებითი სისტემები, როგორიცაა HTTP და HTTPS, ეყრდნობა TCP/IP პროტოკოლებს ინტერნეტში. TCP პროტოკოლი უზრუნველყოფს საიმედო მონაცემთა გადაცემას კლიენტსა და სერვერს შორის ლოგიკური კავშირის გზით, რაც მნიშვნელოვნად ხელს უშლის მონაცემების დაკარგვას, მიუხედავად იმისა ისინი დაშიფრებულია თუ არა. TCP პროტოკოლი მონაცემებს აღიქვამს როგორც ბაიტების მიმდევრობას და თუ ქსელში ხდება მონაცემთა დაკარგვა, ის გადაცემას იმეორებს „მცურავი ფანჯრის“ მეთოდით. IP პროტოკოლი, თავის მხრივ, ეყრდნობა მონაცემთა პაკეტების დეიტაგრამულ გადაცემას ინტერნეტში, და ისიც შეცდომების შემთხვევაში ახორციელებს პაკეტების განმეორებით გადაცემას. TCP/IP სისტემები აქტიურად გამოიყენება კორპორაციულ ქსელებში, სადაც დაცულია როგორც მონაცემთა შეცდომების აღმოჩენის, ისე მათი შესწორების მექანიზმები, რაც პირდაპირ გავლენას ახდენს ინტერნეტის მთლიან უსაფრთხოებაზე (Andrew S. TANENBAUM, Nick FEAMSTER, David WETHERALL, 2021).

უნდა აღინიშნოს, რომ, პროტოკოლების სტეკის ქვემო დონეზე, ინტერნეტში ხშირად გამოიყენება მონაცემთა კოდირების მეთოდები, რომლებიც არა მხოლოდ შეცდომების აღმოჩენას უზრუნველყოფს, არამედ მათი ავტომატურად გასწორების შესაძლებლობას. მაგალითად, ჰემინგის კოდი (Hamming Code) უზრუნველყოფს ბიტური შეცდომის აღმოჩენასა და გასწორებას, ხოლო რიდ-სოლომონის კოდირება (Reed-Solomon Encoding) გამოიყენება პაკეტური შეცდომების შესასწორებლად საკომუნიკაციო არხებში.

TCP/IP პროტოკოლები ძირითადად პასუხისმგებელია მონაცემთა სანდო გადაცემაზე (Data Integrity), მაგრამ არ უზრუნველყოფს მონაცემთა კონფიდენციალურობას ან უსაფრთხოებას. ამან კი გამოიწვია HTTPS შექმნის საჭიროება (Charlie Kaufman, 2023).


H T T P S
H A N D S H A K E
Host 2
Web - სერვერი
(Apache)
HTTP
მისალმება
(SSL/TLS handshake)
ასიმეტრიული მიფრები
(ECC, RSA)
სიმეტრიული მიფრი
(AES GCM)
ძირითადი გზავნილის
მიფრაცია/დეშიფრაცია
(AES GCM)
TCP
IP
SSL
TLS
ინტერნეტი
Host 1
Web - კლიენტი
(Browser)
HTTP
მისალმება
(SSL/TLS handshake)
ასიმეტრიული მიფრები
(ECC, RSA)
სიმეტრიული მიფრი
(AES GCM)
ძირითადი გზავნილის
მიფრაცია/დეშიფრაცია
(AES GCM)
TCP
IP
H A N D S H A K E
H T T P S
Host 2
Web - სერვერი
(Apache)
HTTP
TCP
IP
ინტერნეტი
Host 1
Web - კლიენტი
(Browser)
HTTP
TCP
IP
ა)

სურ. 1, ა

HTTP	Hyper Text Transfer protocol, ჰიპერტესტირების გადაცემის პროტოკოლი
HTTPS	HTTP secure, უსაფრთხო HTTP
SSL	Sequre Sochet Leyar უსაფრთხო სოკეტის შრე
TLS	Trasport Layer Sequrity ტრანსპორტის დონის უსაფრთხოება
ECC	Elyptic Curve Cryptography ელიპტიკურ წირზე დაფუძნებული კრიპტოგრაფია
RSA	ასიმეტრიული კრიპტოგრაფიის მეთოდი
TCP	Transmission Control Protocol
IP	Internet Protocol

ბ) სურ. 1,ბ

როგორც სურ. 1,ბ გვიჩვენებს, SSL/TLS პროტოკოლი მდებარეობს HTTP და TCP პროტოკოლებს შორის, როგორც დამატებითი შრე, რომლის მიზანია კლიენტსა და სერვერს შორის მისალმების პროცესის განხორციელება. ეს პროცესი აუცილებელია შემდეგი ეტაპებისთვის, როდესაც HTTP პროტოკოლებში დაიწყება მონაცემთა გაცვლა სიმეტრიული შიფრაციის ალგორითმების გამოყენებით. ამისთვის, SSL/TLS-ის ფარგლებში გამოიყენება ასიმეტრიული კრიპტოგრაფია ღია გასაღებით, როგორიცაა RSA, დიფ-ჰელმანის ალგორითმი და ECC.

SSL/TLS-ის ძირითადი მიზანია შემდეგი სამი მიზნის მიღწევა:

- კლიენტსა და სერვერს შორის შეთანხმებული შიფრების კრებულების დადგენა;
- კლიენტისა და სერვერის (ხშირად სერვერის) აუთენტიკაცია;
- შიფრაციისა და დეშიფრაციისთვის საჭირო სესიის გასაღების დადგენა.

ამ მიზნის მიღწევა ეფუძნება შიფრისა და შიფრების კრებულის ცნებებს. შიფრი (Cipher) კრიპტოგრაფიაში გამოყენებული ისეთი ალგორითმებია, როგორიცაა, მაგალითად, შიფრაცია, დეშიფრაცია და სხვა. შიფრების კრებული (Cipher Suite) წარმოადგენს შიფრების ერთობლიობაა, რაც მხარეებს შორის კომუნიკაციას უზრუნველყოფს.

განვიხილოთ შიფრების შემდეგი კრებული:

შიფრების ამ კრებულში:

- TLS განსაზღვრავს ბოლო დროს მოქმედ ვერსიებიდან, TLS 1.2 ან TLS 1.3 – ერთ-ერთს.
  - TLS 1.2 ვერსიის გამოყენება რეკომენდებულია ბოლო 15–20 წელია. იგი შეიცავს 37 რაოდენობის შიფრთა კრებულს.
  - TLS 1.3, იგი განახლებული და თვისებრივად გაუმჯობესებული ვერსიაა, მოიცავს შიფრების 5 კრებულს;
- ECDHE (Elliptic Curve Diffie – Hellman Ephemeral) დიფ-ჰელმანის ალგორითმია, რომელიც

იყენებს ელიპტიკურ წირზე დაფუძნებულ კრიპტოგრაფიას და განკუთვნილია ერთჯერადი გამოყენების სიმეტრიული გასაღების შესაქმნელად. საშუალებას იძლევა განხორციელდეს ე.წ. სრულყოფილი ფორვარდული კრიპტოგრაფია (Perfect Forward Cryptography), რაც მედეგია კრიპტანალიზისადმი, რადგან ერთსა და იმავე გასაღებით გზავნილების დაშიფვრა არ ხდება;

- ECDSA (Ellyptic Corve Digital Signature Algorithm) ელიპტიკურ წირზე დაფუძნებული ციფრული ხელმოწერის ალგორითმია და დღეისათვის ითვლება საუკეთესო ალგორითმად;

- AES 128 GCM არის AES (Advanced Encryption Standard) სიმეტრიული შიფრაციის განსაკუთრებულად ეფექტური ალგორითმი, 128- ბიტიანი სიმეტრიული გასაღებით და გალუას მთვლელის მეთოდით (Galois Counter Mode), რაც საშუალებას იძლევა გადაიგზავნოს მონაცემები, რომლებიც როგორც კონფიდენციალურ, დასაშიფრავ, ისე ღია ტექსტით გადასაცემ ნაწილებს შეიცავს;

- SHA 256 კრიპტოგრაფიული ჰეშირების ალგორითმია, რომელიც გამოიყენება როგორც ციფრული ხელმოწერის, ისე მონაცემთა გადაცემის სისწორის კონტროლის საკითხებში.

როდესაც კლიენტსა და სერვერს შორის მიმდინარეობს კომუნიკაცია, შეიძლება გამოყენებული იყოს მხოლოდ რამდენიმე ალგორითმი, მათ შორის ინსტალირებულ შიფრთა კრებულებიდან. ამიტომ, საჭიროა გაირკვეს, რომელი რეკომენდებული კრებულებია ხელმისაწვდომი ორივე მხარისთვის და შეირჩეს საერთო კრებული მონაცემთა გაცვლისთვის (Nakov, 2018). ბოლო პერიოდში ყველაზე გავრცელებული TLS პროტოკოლის ვერსიებია: TLS 1.2 და TLS 1.3. TLS 1.2 მოიცავს 37 სხვადასხვა შიფრზე დაფუძნებულ კრებულს, ხოლო TLS 1.3, რომელიც TLS 1.2-ის განახლებული და გაუმჯობესებული ვერსიაა, მხოლოდ 5 კრებულს, როგორც ეს მოცემულია ნახ-2 სურათზე.

37 კრებული

1.	TLS 1.2	ECDHE	ECDSA	AES_128_GCM	SHA256
2.	TLS 1.2	ECDHE	ECDSA	AES_256_GCM	SHA384
.					
.					
.					
36.	TLS 1.2	DHE	RSA	AES_128_CBC	SHA256
37.	TLS 1.2	DHE	RSA	AES_256_CBC	SHA256

ა)

5 კრებული

1.	TLS 1.3	ECDHE	ECDSA	AES_256_GCM	SHA384
2.	TLS 1.3	ECDHE	ECDSA	CHACHA20_POLY1305	SHA256
3.	TLS 1.3	ECDHE	ECDSA	AES_128_GCM	SHA256
4.	TLS 1.3	ECDHE	ECDSA	AES_128_CCM_8	SHA256
5.	TLS 1.3	ECDHE	ECDSA	AES_128_CCM	SHA256

ბ)

სურ. 2

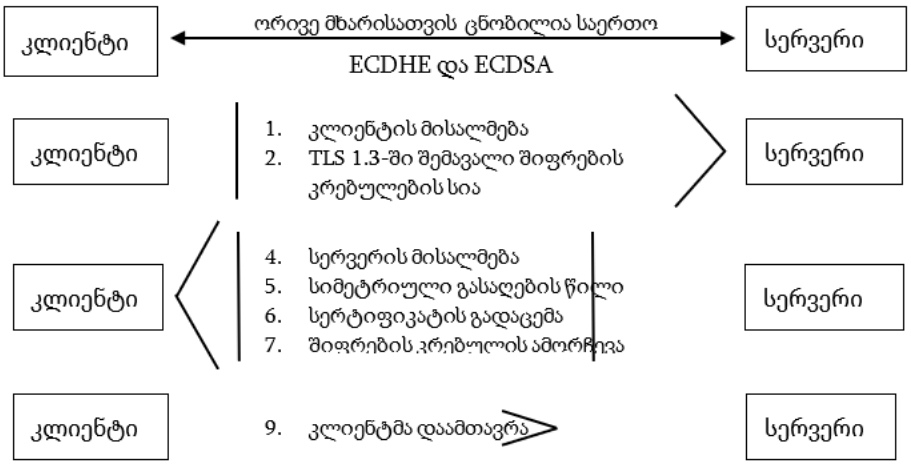
როგორც სურათი გვიჩვენებს, TLS 1.2-ში თითოეული შიფრთა კრებული მოიცავს 5 მახასიათებელს და 37 კრებულს, რომელთა შორის ზოგი შეიძლება იყოს მოძველებული და კვლავ შენარჩუნებული ბრაუზერებსა და სერვერებში. TLS 1.3-ის შემთხვევაში კი მხოლოდ 5 კრებულია განსაზღვრული და ყველა მათგანი იყენებს ECDHE და ECDSA შიფრებს, რაც პროცესს ამარტივებს. (სურათზე ეს წარმოდგენილია წყვეტილ ხაზებში მოქცეული ელემენტებით). დამატებით, ელიპტიკური კრიპტოგრაფიის

გამოყენება ხელს უწყობს სრულყოფილი ფორვარდული საიდუმლოს განხორციელებას ECDHE-ს გამოყენებით და ECDSA-ს დახმარებით მიღწეულ სწრაფქმედებას (Nohe, 2019), (Corbellini, 2015).

ამგვარად, კლიენტსა და სერვერს შორის კომუნიკაციისთის საჭიროა როგორც კლიენტს, ისე სერვერს ინსტალირებული ჰქონდეს ერთი საერთო კრებული მაინც. რადგან TLS 1.3-ში შემავალ კრებულებს ყველას აქვს ერთი და იგივე ორი საერთო ელემენტი (სურ. 2, ბ) ECDHE და ECDSA, მისალმებისას მათი გაცვლა საჭირო აღარ არის და ხდება კრებულებში შემავალი დანარჩენი 2 ელემენტის გაცვლა. ამგვარად, ვღებულობთ ცხრილს:

TLS 1.3	AES_256_GCM	SHA384
TLS 1.3	CHACHA20_POLY1305	SHA256
TLS 1.3	AES_128_GCM	SHA256
TLS 1.3	AES_128_CCM_8	SHA256
TLS 1.3	AES_128_CCM	SHA256

განვიხილოთ კლიენტ-სერვერული ურთიერთობა დროში, როცა კომუნიკაციის წამომწყებია კლიენტი (სურ. 3).



სურ. 3

კლიენტის მხარე

1. კლიენტი იწყებს კომუნიკაციას მისალმებით;

2. კლიენტი სერვერს გადასცემს TLS 1.3 პროტოკოლით გათვალისწინებულ იმ კრებულების სიას, რომელიც მას ინსტალირებული აქვს. სერვერი ადარებს გადმოცემულ სიაში არსებული შიფრების კრებულებს სერვერში ინსტალირებული კრებულების ჩამონათვალს და, საერთო ელემენტების აღმოჩენის შემთხვევაში ახდენს საუკეთესოს არჩევას, რაც ოპერაციის წარმატებით დამთავრებაზე მიუთითებს.

3. კლიენტი იყენებს დიფ-ჰელმანის ალგორითმებს და განსაზღვრავს თავის წილ მონაცემს, რომელიც გამოიყენება სიმეტრიული შიფრაციის გასაღების განსაზღვრის პროცედურაში (ნ. ლომინაძე,

თ. ლომინაძე, თ. ასათიანი, რ. პაპიაშვილი. კრიპტოგრაფიის საფუძვლები, პარაგრაფი დიფ-ჰელმანის ალგორითმი ელიპტიკური წირისათვის).

სერვერის მხარე

4. სერვერის მისალმება კლიენტს მიანიშნებს, რომ იწყებს მონაცემის გადაცემას.

5. კლიენტი იყენებს დიფი-ჰელმანის ალგორითმს და განსაზღვრავს თავის წილ მონაცემს სიმეტრიული გასაღების განსაზღვრისათვის.

6. კლიენტისაგან სერტიფიკატის გადაცემა მისი ვალიდურობის შემოწმების მიზნით.

7. შიფრების კრებულის ამორჩევა.

8. სერვერმა დაამთავრა.

ამგვარად, მისალმების პროცედურების დასრულების შემდეგ როგორც კლიენტი, ისე სერვერი ფლობს სიმეტრიული შიფრაციისათის აუცილებელ სიმეტრიულ გასაღებს და ხდება ძირითადი გზავნილის გადაგზავნა დაშიფრული ფორმით სიმეტრიული შიფრაციის ალგორითმის, მაგალითად, AES_256_GCM გამოყენებით (ნ. ლომინაძე, თ. ლომინაძე, თ. ასათიანი, რ. პაპიაშვილი. კრიპტოგრაფიის საფუძვლები, თავი 4).

დასკვნა

შეიძლება ითქვას, რომ მისალმების ოპერაციებში გამოყენებულია დიფ-ჰელმანის და ელიპტიკურ წირზე დაფუძნებული ასიმეტრიული შიფრაციის ალგორითმები, რაც უზრუნველყოფს კლიენტ-სერვერული მისალმების ეფექტურად და საიმედოდ ჩატარებას.

ლიტერატურა

1. Tanenbaum, A. S., Feamster, N., & Wetherall, D. (2021). *Computer networks*. Pearson Education.
2. Kaufman, C., Perlman, R., & Speciner, M. (2023). *Network security: Private communication in a public world*. Pearson Education, Inc.
3. Lominadze, N., Lominadze, T., Asatiani, T., & Papiashvili, R. (2024). *Fundamentals of cryptography* [In Georgian]. Tbilisi: Scientific Center "IT Consulting" at GTU. https://gtu.ge/ims/pdf/cyptography.pdf
4. Mdzinarishvili, L., Kachakhidze, N., Ugulava, D., & Khomeriki, N. (2018). *Discrete mathematics* [In Georgian]. Publishing House "Technical University".
5. Corbellini, A. (2015, May 17). *Elliptic curve cryptography: A gentle introduction*. https://andrea.corbellini.name/2015/05/17/elliptic-curve-cryptography-a-gentle-introduction/#scalar-multiplication
6. Nakov, S. (2018). *Practical cryptography for developers*. Sofia: MIT License. https://github.com/nakov/practical-cryptography-for-developers-book
7. Nohe, P. (2019, April 30). *Taking a closer look at the SSL/TLS handshake*. https://www.thesslstore.com/blog/explaining-ssl-handshake

UDC 513.21
SCOPUS CODE 1700
https://doi.org/10.36073/1512-0996-2025-1-392-400

The use of Symmetric and Asymmetric Encryption in Cybersecurity

Nodar lominadze Department of Information Technologies, Georgian Technical University, Georgia, 0160, Tbilisi, 69, M. Kostava str.
E-mail: n.lominadze@gtu.ge

Tamar lominadze Department of Information Technologies, Georgian Technical University, Georgia, 0160, Tbilisi, 69, M. Kostava str.
E-mail: t.lominadze@gtu.ge

Tamar Asatiani Department of Information Technologies, Georgian Technical University, Georgia, 0160, Tbilisi, 69, M. Kostava str.
E-mail: t.asatiani@gtu.ge

Reviewers:

R. Kakubava, Professor, Faculty of Informatics and Control Systems, GTU
E-mail: r.kakubava@gtu.ge
I. Kartvelishvili, Professor, Faculty of Informatics and Control Systems, GTU
E-mail: s.kartvelishvili@gtu.ge

Abstract. The development of information security systems and increasing their efficiency can be considered on the example of HTTPS, which is an improved version of the HTTP protocol. HTTPS provides data protection during communication. The use of TCP / IP protocols over the internet is the basis for reliable data transmission, although they cannot guarantee data privacy. This requires an additional security layer, such as the SSL/TLS protocol, which provides secure connections between the client and the server. SSL/TLS protocols are one of the important technologies. Its use of encryption and decryption algorithms between client and server protects the connection from criminal interference. This process is based on mathematical models and algorithms that constantly need updating to be able to respond to modern cybersecurity challenges. The article discusses the issues of improving the efficiency rate of client-server relationship characteristics in a computer based on rational selection of cipher suites. The issues of using elliptic circle-based cryptography are highlighted, such as ECDHE (elliptic circle-based Diffie-Hellman ephemeral algorithm) and ECDSA (elliptic circle-based digital signature algorithm), which allows to reduce the number of ciphers used on the one hand and at the same time improve the communication characteristics of the computer network.

Keywords: Eliptic curve Cryptography, ECC; Elliptic Curve Diffie – Hellman Ephemeral ECDHE; Elliptic Curve Digital Singonture Algorithm ECDSA; HTTP Sequre; TLS.

განხილვის თარიღი 10.02.2005
შემოსვლის თარიღი 27.02.2025
ხელმოწერილია დასაბეჭდად 25.03.2025