PD.TVZ.HR
POLYTECHNIC & DESIGN Vol. 10, No. 3, 2022.
Mrežna inačica: ISSN 2459-6302
Tiskana inačica: ISSN 1849-1995
DOI: 10.19279/TVZ.PD.2022-10-3-05

HIBRIDNI KRIPTOSUSTAVI U KLIJENTSKO-POSLUŽITELJSKOJ ARHITEKTURI NA APLIKACIJSKOM SLOJU INTERNETA

HYBRID CRYPTOSYSTEMS IN CLIENT-SERVER ARCHITECTURE ON THE APPLICATION LAYER OF THE INTERNET

Mirna Pibernik[1], Željko Kovačević[2]

[1]Tehničko veleučilište u Zagrebu, Vrbik 8, 10000 Zagreb, Hrvatska, Studentica
[2]Tehničko veleučilište u Zagrebu, Vrbik 8, 10000 Zagreb, Hrvatska

SAŽETAK

Uslijed sve šire upotrebe kriptografije u raznim domenama računarstva razvijaju se sve napredniji kriptografski algoritmi, protokoli i sustavi o čijoj ispravnosti ovisi povjerljivost privatne i poslovne komunikacije sve većeg broja ljudi. Povrh kompleksnosti svake od kriptografskih komponenti, moderne klijentsko-poslužiteljske arhitekture zahtijevaju njihove precizno izvedene kombinacije s drugim elementima sustava koji također primjenjuju kriptografiju u različite svrhe. S ciljem boljeg razumijevanja uloge kriptografskih primitiva u suvremenim distribuiranim sustavima, u ovom su radu objedinjene značajke temeljnih kriptografskih metoda zajedno s njihovim primjenama na aplikacijskom sloju Interneta. Na primjerima popularnih hibridnih kriptosustava (Transport Layer Security, Secure Shell, End-to-end Encryption) predstavljene su namjene kriptografije u distribuiranim mrežnim aplikacijama uz sažet opis glavnih ideja koje se koriste pri oblikovanju takvih sustava. Rad ne ulazi u tehničke detalje i implementacije algoritama, već doprinosi jezgrovit pregled navedenih principa i ideja uz praktične primjere relevantne mladim programskim inženjerima.

Ključne riječi: *hibridni kriptosustav, klijentsko-poslužiteljska arhitektura, informacijska sigurnost, kriptografija*

ABSTRACT

Due to the increasing use of cryptography in various domains of computing, more and more advanced cryptographic algorithms, protocols, and systems are being developed, the correctness of which largely determines the confidentiality of private and business communication of an increasing number of people. In addition to the complexity of each of the cryptographic components, modern client-server architectures require their precisely executed combinations with other elements of the system that also apply cryptography for various purposes. In order to better understand the role of cryptographic primitives in modern distributed systems, this paper combines the features of basic cryptographic methods together with their applications on the application layer of the Internet. Examples of popular hybrid cryptosystems (Transport Layer Security, Secure Shell, End-to-end Encryption) present the purposes of cryptography in distributed network applications with a brief description of the main ideas used in designing such systems. The paper does not go into technical details and implementations of algorithms but contributes a concise overview of these principles and ideas with practical examples relevant to young software engineers.

Keywords: *hybrid cryptosystem, client-server architecture, information security, cryptography*

1. UVOD
1. INTRODUCTION

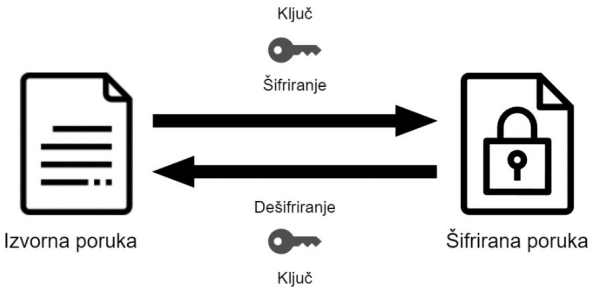
Informacijska sigurnost na Internetu u počecima njegovog razvoja nije bila prioritet [1] [2]. Potreba za poboljšanjem sigurnosti javlja se ranih devedesetih godina prošlog stoljeća porastom popularnosti usluga poput internetske trgovine, internetskog bankarstva i sličnih aplikacija koje obrađuju veliku količinu povjerljivih transakcija na javnoj mreži [2] [3]. Uzimajući u obzir slojevitu strukturu Interneta i raznolikost komunikacijskih protokola koji ga sačinjavaju, iznađeni su brojni pristupi za osiguravanje komunikacije na javnoj mreži s različitim svrhama i karakteristikama [4] [5]. Mnogi od njih koriste tehnike kriptografije. Kriptografija izučava matematičke postupke za postizanje osnovnih ciljeva informacijske sigurnosti poput povjerljivosti, integriteta i autentifikacije izvora podataka [6]. Pojam kriptosustav označava "set kriptografskih primitiva za pružanje usluga informacijske sigurnosti" [6], a kriptografski primitivi (alati) uključuju funkcije sažimanja te sustave šifriranja i digitalnog potpisa [6]. Svrha je ovog rada u sažetom obliku predstaviti temeljna načela i praktične primjene kriptosustava s kojima se danas susreću inženjeri klijentsko-poslužiteljskih web aplikacija, a glavni su doprinosi jezgrovitost i objedinjenost oprimjerenih kriptografskih koncepata relevantnih za ovu ciljnu skupinu. Rad posebno doprinosi pregled navedenih tema jednostavnim jezikom i ilustracijama čime olakšava sagledavanje šire slike upotrebe kriptografije u suvremenim aplikacijama. Time nastoji približiti kriptografsku znanost mladim programskim inženjerima kako bi uz njenu pomoć dizajnirali i razvijali kvalitetnije i sigurnije aplikacije. U tom se kontekstu, pored navedenih osnovnih ciljeva informacijske sigurnosti, korištenjem kriptosustava nastoji postići i neporecivost (eng. non-repudiation), unaprijedna tajnost (eng. forward secrecy) [4], sigurnost nakon kompromisa (eng. post-compromise security) [7], te zaštita od napada čovjek u sredini (eng. man-in-the-middle attack), napada ponavljanja (eng. replay attack) i drugih [1] [8].

Primjenu kriptografije nalazimo još prije 4000 godina u Egiptu, a 20. stoljeće bilo je razdoblje ubrzanog napretka i standardizacije kriptografskih mehanizama usporedno s razvojem informacijsko-komunikacijskih tehnologija [6]. Matematički alati modernih kriptosustava formalizirani su u radovima znanstvenika poput W. Diffie i M. E. Hellman (1976.), R. Rivest, A. Shamir i L. Adleman (1978.), T. Elgamal (1985.) [6]. Prvi značajan kriptografski standard u širokoj upotrebi, Data Encryption Standard, donesen je 1977. godine u Sjedinjenim Američkim Državama [9], 1987. prihvaćen je međunarodni kriptografski standard blok šifri ISO/IEC 8372, a 1991. međunarodni standard za digitalni potpis ISO/IEC 9796 [6]. Krajem 1992. Internet Engineering Task Force (IETF) započinje razvoj okvira IPsec [10] da bi 1995. RFC 1825-1829 definirali temelje kriptografskih protokola za sigurnost mrežnog sloja modela OSI [1] [4]. Iste godine tvrtka Netscape razvija paket Secure Sockets Layer (SSL) koji se postupno unapređuje i postaje standardiziran kao Transport Layer Security (TLS), hibridni kriptosustav čija se najnovija inačica 1.3 prihvaćena 2018. danas koristi [1] [11].

2. SIMETRIČNI KRIPTOSUSTAVI (KRIPTOSUSTAVI S TAJNIM KLJUČEM)
2. SYMMETRIC CRYPTOSYSTEMS (SECRET-KEY CRYPTOSYSTEMS)

Simetrična kriptografija osnovna je vrsta kriptografije, korištena od začetka discipline [1]. Bavi se formuliranjem algoritama koji omogućuju šifriranje poruke na način da ju može dešifrirati samo posjednik ključa. Šifriranje je proces transformacije poruke funkcijom koja je parametrizirana ključem [1]. Kao što to prikazuje Slika 1, u simetričnoj kriptografiji koristi se jedan ključ za šifriranje i dešifriranje [12]. Razlika između lozinke i kriptografskog ključa u kriptografskoj je snazi: kriptosustav parametriziran lozinkom koju korisnik pamti lakše je razbiti nego kriptosustav parametriziran kriptografskim ključem [12]. Lozinku je moguće transformirati u ključ koji ima poželjna kriptografska svojstva (visoka konfuzija i difuzija) specijaliziranom kriptografskom funkcijom [8] [12]. Moderni algoritmi simetrične kriptografije vrlo su učinkoviti s obzirom na brzinu izračuna

i dužinu ključa potrebnu za visoku razinu sigurnosti. Dugogodišnjim razvojem simetričnih kriptosustava algoritmi simetrične kriptografije su standardizirani (npr. Advanced Encryption Standard/AES) što je dovelo do veće pouzdanosti (smanjen rizik od pogrešne implementacije) i brzine (AES instrukcije ugrađene su u brojne moderne procesore) [1] [8].



Slika 1 *Načelo rada simetričnog kriptografskog algoritma*

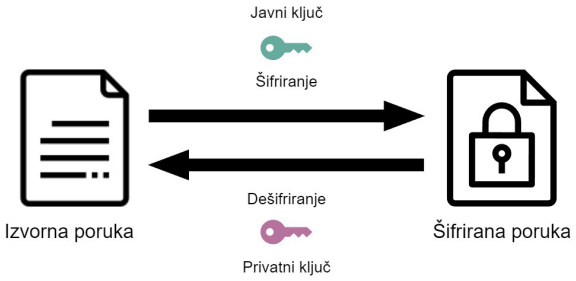
Figure 1 *Working principle of symmetric cryptographic algorithm*

Međutim, da bi svrha šifriranja (tajnost poruke) bila ostvarena, ključ mora ostati tajan. Kod isključivo simetričnog kriptosustava javlja se problem distribucije ključa [6] na nesigurnom komunikacijskom kanalu poput Interneta: kako postići da ključ bude poznat strankama koje komuniciraju, a drugima ne? Na ovo pitanje odgovaraju asimetrični kriptosustavi.

3. ASIMETRIČNI KRIPTOSUSTAVI (KRIPTOSUSTAVI S JAVNIM KLJUČEM)

3. ASYMMETRIC CRYPTOSYSTEMS (PUBLIC-KEY CRYPTOSYSTEMS)

Asimetrična kriptografija (kriptografija javnog ključa) rješava problem distribucije ključa putem nesigurnog kanala [1] [4] [8]. U širokoj su upotrebi dva pristupa rješenju tog problema, predstavljena dvjema skupinama kriptografskih algoritama [4]. U prvu skupinu svrstavamo kriptosustave poput RSA koji problem distribucije ključa rješavaju tako da se umjesto jednog ključa koriste dva (par ključeva). Ovakav kriptosustav omogućuje generiranje dvaju ključeva koji su matematički povezani tako da je sadržaj šifriran jednim ključem iz para moguće dešifrirati jedino drugim ključem iz istog para. Ovakav kriptosustav također osigurava da je iz jednog (tzv. privatnog) ključa vrlo teško u razumnom vremenu izvesti drugi (tzv. javni) ključ iz para. Zbog ovih je svojstva moguće jedan od ključeva iz para (javni ključ) distribuirati nesigurnim kanalom bez narušavanja sigurnosti šifriranja tim ključevima, pod uvjetom da drugi ključ iz para ostane tajan (privatni ključ) [12]. Slika 2 ilustrira načelo rada ove skupine algoritama. U drugoj su skupini kriptosustavi poput Diffie-Hellman koji problem distribucije ključa rješavaju tako da stranke prilikom uspostave komunikacije na nesigurnom kanalu zajednički generiraju ključ kojeg potom koriste za šifriranje poruka u toj sesiji [4]. Asimetrični kriptosustav jamči da je trećoj strani vrlo teško u razumnom vremenu izvesti taj ključ iz informacija koje su komunicirane nesigurnim kanalom [12]. Primjerice, faktorizacija RSA-768 trajala je dvije godine uz pomoć oko 1000 procesorskih jezgri [13]. Pretpostavlja se da bi na istim računalima za faktorijalizaciju RSA-1024 trebalo oko 7481 godina. RSA se također danas može koristiti i inačicama od 2048 i 4096 bita.

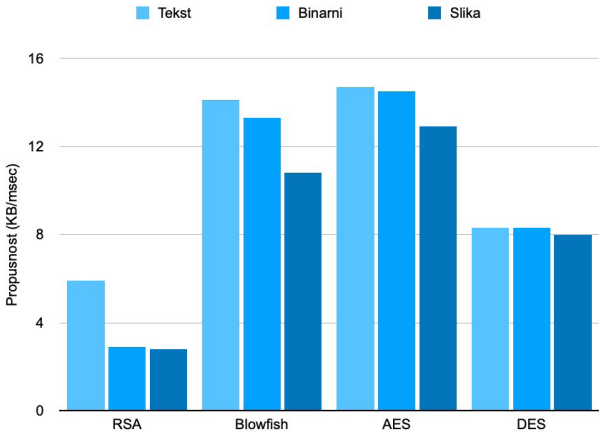


Slika 2 *Načelo rada asimetričnog kriptografskog algoritma*

Figure 2 *Working principle of asymmetric cryptographic algorithm*

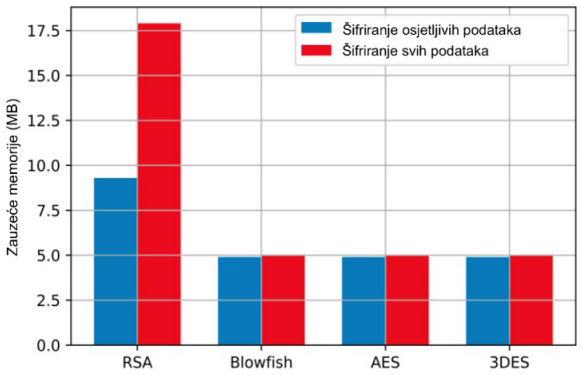
S obzirom na zahtjevnost postizanja navedenih svojstava javnih ključeva, matematički izračuni korišteni u implementacijama algoritama asimetrične kriptografije traže više procesorskih resursa od algoritama simetrične kriptografije [8]. Slika 3 prikazuje usporedbu propusnosti popularnih kriptosustava: asimetrični algoritam RSA ima otprilike dvostruko manju propusnost pri šifriranju tekstualnih podataka od najbržeg uspoređivanog simetričnog algoritma (AES), te otprilike tri puta manju propusnost pri šifriranju binarnih i slikovnih podataka [14]. Osim manje brzine, komparativni nedostatak asimetrične

kriptografije je i veća dužina ključa potrebna zbog njegove javnosti: ključevi trenutno najkorištenijeg asimetričnog kriptosustava RSA pet do deset puta su duži od simetričnog ključa kriptografski ekvivalentne snage, a noviji asimetrični algoritmi temeljeni na eliptičnim krivuljama koriste ključ dvostruko duži od ekvivalentnog simetričnog [1] [6]. Asimetrični kriptosustav zahtijeva i gotovo dvostruko više radne memorije od simetričnog, što prikazuje Slika 4. Stoga nastojimo smanjiti potrebu za generiranjem, transportom i pohranom asimetričnih ključeva.



Slika 3 *Usporedba propusnosti odabranih simetričnih i asimetričnih kriptosustava.*

Figure 3 *Throughput comparison of selected symmetric and asymmetric cryptosystems.*



Slika 4 *Usporedba zauzeća memorije odabrani simetričnih I asimetričnih kriptosustava. Izvor: Prilagođeno [15]*

Figure 4 *Memory consumption comparison of selected symmetric and asymmetric cryptosystems.*

Iako javnost ključa ne umanjuje njegovu kriptografsku snagu (zahtjevnost razbijanja kriptosustava), sustavi klijentsko-poslužiteljske arhitekture sa sobom povlače sigurnosne izazove koji proizlaze iz njihove distribuiranosti. Među najvažnijima su dva donekle povezana problema: tajnost privatnog ključa i identitet sugovornika (svrha kriptosustava, povjerljivost komunikacije, ostvarena je samo ako je željena stranka posjednik privatnog ključa) [6]. Pristupi njihovim rješenjima u suvremenim distribuiranim aplikacijama uključuju hibridne kriptosustave.

4. HIBRIDNI KRIPTOSUSTAVI NA INTERNETU

4. HYBRID CRYPTOSYSTEMS ON THE INTERNET

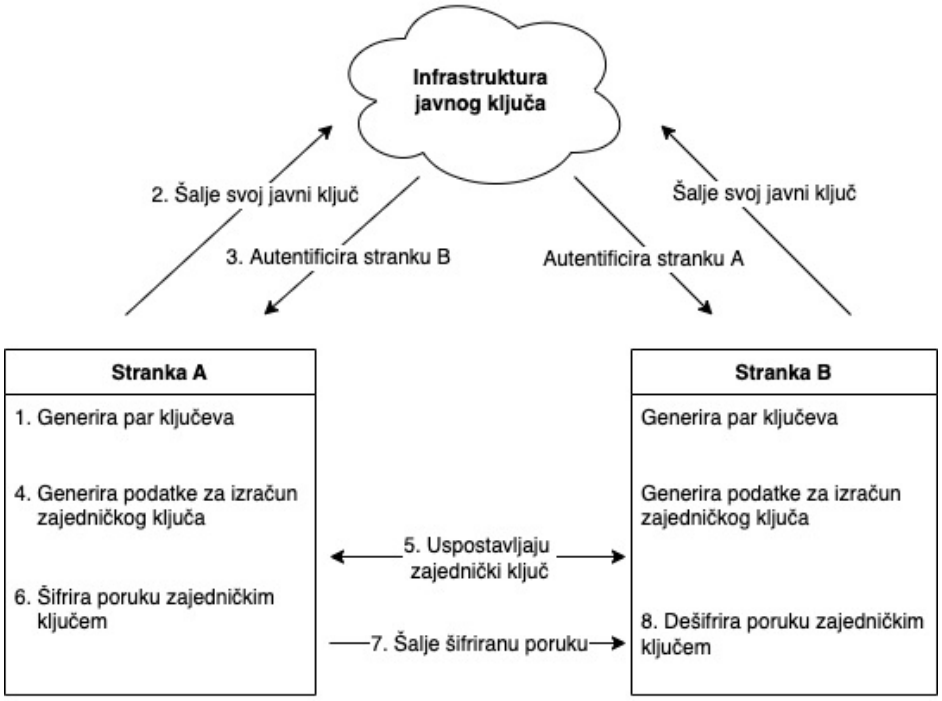
Hibridni kriptosustavi za postizanje ciljeva navedenih u uvodu ovog rada koriste mehanizme kojima kombiniraju poželjne značajke simetričnih (brzina izračuna, dužina ključa) i asimetričnih kriptosustava (distribucija ključa) te nastoje riješiti probleme kojima se ti sustavi sami po sebi ne bave (tajnost privatnog ključa i identitet sugovornika). Ti se mehanizmi sastoje od kriptografskih protokola i popratne infrastrukture čija integracija u distribuirane internetske aplikacije ne smije narušiti temeljne značajke tih aplikacija kao što su skalabilnost i dostupnost.

4.1. ELEMENTI KRIPTOGRAFSKIH PROTOKOLA

Kriptografski protokoli na aplikacijskom sloju Interneta oslanjaju se na podatkovni tok s nižeg (transportnog) sloja čija je obrada izvan opsega ovog članka. Kriptografski protokoli, nazivani i „distribuirani algoritmi“, nerijetko su i sami sastavljeni od više slojeva ili podprotokola, a svaki sloj od više koraka u kojima se koriste kriptografski primitivi [6]. *Kriptografske funkcije sažimanja* koriste se za osiguranje integriteta poruke simetričnim kriptosustavom (MAC algoritmi, *key derivation* funkcije) ili u kombinaciji s asimetričnim kriptosustavom digitalnog potpisa [6]. *Digitalni potpis* kriptografski je alat koji digitalnim dokumentima pridaje svojstva vlastoručnog potpisa (autentifikacija i neporecivost). Za digitalni potpis najčešće se koristi asimetrični

kriptosustav, npr. RSA ili Digital Signature Algorithm (DSA) [1] [12]. *Uspostavljanje zajedničkog ključa* (eng. *key establishment/ negotiation*) vrsta je kriptografskog protokola u kojem stranke uspostavljaju zajednički ključ (eng. *shared secret*) za šifriranje komunikacije u svojoj sesiji simetričnim kriptosustavom. Često se javlja u kombinaciji s autentifikacijom asimetričnim kriptostavom, kako bi stranke na nesigurnom kanalu mogle utvrditi identitet sugovornika, pri čemu se javni ključ pribavlja kroz infrastrukturu javnog ključa. Takva ispravno implementirana kombinacija, u kojoj se zajednički ključ redovito obnavlja, štiti od *man-in-the-middle* i *replay* napada te pruža *forward-secrecy* i *post-compromise security*. Infrastruktura javnog ključa (eng. *Public Key Infrastructure*) služi za utvrđivanje identiteta uz pomoć certifikata. *Certifikat* sadrži javni ključ stranke koju identificira te dodatne podatke poput vremenskog raspona u kojem je certifikat važeći, naziv i digitalni potpis izdavatelja certifikata i dr. (najkorišteniji je X.509 standard) [1]. Za klijentsko-poslužiteljske aplikacije najčešće se koristi potpuno centralizirana (uslugu autentifikacije pružaju tzv. *trusted third party* entiteti kao što su Certificate Authority i Key Distribution Center) ili djelomično centralizirana infrastruktura javnog ključa (npr. sustav Web of Trust). Tehnike *upravljanja ključevima* (eng. *key management*) bave se generiranjem, upravljanjem životnim ciklusom, pohranom i čuvanjem tajnosti privatnih te distribucijom javnih ključeva. Uspostavljanje zajedničkog ključa i infrastrukturu javnog ključa možemo svrstati u tehnike upravljanja ključevima [6] [8]. Jednu od mogućih kombinacija ovih elemenata prikazuje Slika 3.

U 1. i 2. koraku primjera sa slike koristi se asimetrični kriptosustav poput RSA koji generira dva povezana ključa. Idući korak uključuje korištenje certifikata koji sadržava javni ključ stranke koju se autentificira i digitalni potpis *trusted third party* entiteta, uz primjenu kriptografskih funkcija sažimanja. Nakon utvrđivanja identiteta sugovornika, u 4. i 5. koraku koristi se asimetrični kriptosustav poput Diffie-Hellman, pri čemu stranke na nesigurnom kanalu izmjenjuju podatke za izračun zajedničkog ključa [16]. Taj se ključ koristi za šifriranje i dešifriranje poruke u 6. i 8. koraku, također često uz primjenu kriptografskih funkcija sažimanja, čime je komunikacija na nesigurnom kanalu u 7. koraku osigurana. Obje stranke zasebno na svojim uređajima primjenjuju tehnike upravljanja ključevima prije, za vrijeme i nakon ove komunikacije.



Slika 5 *Primjer načela rada hibridnog kriptosustava na Internetu. Dijagram prikazuje situaciju u kojoj je pošiljatelj poruke stranka A, a primatelj stranka B.*

Figure 5 *An example of how a hybrid cryptosystem works on the Internet. The diagram shows a situation in which the sender of the message is party A and the recipient is party B*

4.2. PRIMJERI HIBRIDNIH KRIPTOSUSTAVA NA INTERNETU

Transport Layer Security (TLS) je protokol za uspostavljanje komunikacijskog kanala dviju stranki koji pruža povjerljivost, integritet i autentifikaciju [17]. Unatoč nazivu, TLS ne pripada transportnom sloju, nego se nalazi iznad njega (kao zasebni sloj ili unutar aplikacijskog sloja) [18]. Najistaknutija je primjena TLS-a za osiguravanje komunikacije putem HTTP-a (*HTTP over TLS* ili HTTPS), a koristi se i kao podloga za email, udaljeni rad (*remote desktop*), VoIP, VPN i druge mrežne aplikacije. Protokol ima dvije komponente: (1) uspostavljanje sigurnog kanala (*Handshake Protocol*) i (2) korištenje tog kanala (*Record Protocol*). Na početku komunikacije odvija se (1) u sklopu kojeg stranke utvrđuju inačicu protokola i parametre simetričnog kriptosustava kojeg će koristiti u nastavku sesije, a moguća je i autentifikacija jedne ili obiju stranaka. U slučaju HTTPS-a uglavnom se autentificira samo poslužitelj (stranka koja nije započela sesiju) pomoću centralizirane infrastrukture javnog ključa. Nakon uspostavljanja sigurnog kanala, on se koristi za komunikaciju (2) koja je šifrirana simetričnim kriptosustavom sa zajedničkim ključem [11].

Secure Shell (SSH) kriptografski je alat koji se može koristiti kao protokol za uspostavu povjerljivog komunikacijskog kanala, klijentsko-poslužiteljska aplikacija ili komandno sučelje. Protokol se sastoji od triju komponenti: (1) pruža autentifikaciju poslužitelja, uspostavu zajedničkog ključa i zaštitu integriteta uz unaprijednu tajnost (*forward secrecy*) (*Transport Layer Protocol*), (2) pruža autentifikaciju klijenta (*User Authentication Protocol*), i (3) preusmjerava podatkovni tok sigurnog komunikacijskog kanala uspostavljenog komponentama (1) i (2) u ciljni kanal (*Connection Protocol*) [19]. Komponenta (1) ima sličnu funkcionalnost kao TLS, ali nije neuobičajeno koristiti SSH i TLS zajedno. Najistaknutija je primjena SSH za osiguravanje daljinskog izvršavanja naredbi, a koristi se i kao podloga za prijenos datoteka, VPN i proxy uslugu [20].

Protokoli za slanje trenutačnih poruka (eng. *instant messaging*) posljednjih godina u svoju arhitekturu uvode kriptografske komponente i pružaju uslugu šifriranja s kraja na kraj (eng. *end-to-end encryption/E2EE*). Aplikacija na klijentskom uređaju šifrira i dešifrira poruke te obavlja jedan dio upravljanja ključevima, a poslužitelj prenosi šifrirane poruke i obavlja drugi dio upravljanja ključevima. Ova vrsta protokola kompleksnija je od prethodnih dvaju primjera jer treba podržavati asinkronu i grupnu komunikaciju. Popularni primjeri protokola E2EE su iMessage i Signal [21]. Stariji od ovih dvaju protokola, iMessage, zatvorenog je koda (eng. *closed source/ proprietary*) i koristi poslužitelje tvrtke Apple kao infrastrukturu javnog ključa [22]. Signal protokol otvorenog je koda koji je podvrgnut znanstvenim analizama i trenutno se koristi u aplikacijama poput WhatsApp, Facebook Messenger, Viber i Signal [23] [24] [25] [26].

5. ZAKLJUČAK
5. CONCLUSION

Kriptografija općenito štiti povjerljivost podataka. Podupire protokole za provjeru autentičnosti i digitalne certifikate te bi bez njene upotrebe bilo teško osigurati komunikacijske protokole i zaštiti pristup resursima i podacima. Važnost i dobrobiti kriptografije i postojećih kriptosustava vidljive su i u svakodnevnom životu pri radu s osobnim dokumentima. Umjesto odlaska u zgrade državnih institucija i čekanja u redovima za dokumente, pojedinci se mogu autorizirati iz udobnosti svog doma koristeći zaštićene protokole i pristupiti portalima državnih institucija kako bi dobili digitalno potpisane dokumente koji su pravno jednako valjani kao da su vlastoručno potpisani. Upravo zbog toga u ovom smo radu pružili pregled nekih od najvažnijih kriptosustava, protokola i alata, te opisali njihovu primjenu na Internetu. Osim u klasičnoj internetskoj komunikaciji, primjena kriptosustava prisutna je i u Internetu stvari (eng. Internet of Things - IoT). Uzimajući u obzir trenutnu zahtjevnost postojećih kriptosustava u pogledu implementacije i izvođenja te ograničenja platforme IoT (dostupna memorija, brzina, kapacitet baterije itd.) u našem budućem radu planiramo istražiti „lagane“ (eng. lightweight) kriptografske algoritme koji su po svojoj implementaciji i zahtjevima za izvođenje namijenjeni za izvršavanje na platformi IoT.

6. REFERENCE
6. REFERENCES

[1.] A. S. Tanenbaum, N. Feamster i D. Wetherall, Computer Networks (6th Edition), Harlow: Pearson Education Limited, 2021., ISBN: 9780136764052

[2.] J. Naughton, A Brief History of the Future: The origins of the internet, London: Orion Books Ltd., 2001, p. 269., ISBN: 9780753810934

[3.] The Editors of Encyclopaedia Britannica, »Britannica,« 10 2 2016. [Mrežno]. Available: https://www.britannica.com/technology/e-commerce. [Pokušaj pristupa 9 3 2022].

[4.] C. Kaufman, R. Perlman i M. Speciner, Network Security: Private Communication in a Public World (2nd Edition), Chennai: Pearson India Education Services Pvt. Ltd, 2017., ISBN: 9780130460196

[5.] D. E. Comer, Computer Networks and Internets (6th Edition), Essex: Pearson Education Limited, 2015., ISBN: 9780133587937

[6.] A. J. Menezes, P. C. van Oorschot, Vanstone I A. Scott, Handbook of Applied Cryptography, Boca Raton: CRC Press (Taylor & Francis Group), 2001., ISBN: 0-8493-8523-7

[7.] K. Cohn-Gordon, C. Cremers I L. Garratt, »On Post-compromise Security,« u 2016 IEEE 29th Computer Security Foundations Symposium (CSF), 2016., doi:10.1109/CSF.2016.19

[8.] N. Ferguson, B. Schneier I T. Kohno, Cryptography Engineering: Design Principles and Practical Applications, Indianapolis: Wiley Publishing, Inc., 2010., ISBN: 978-0470474242

[9.] W. Diffie i M. E. Hellman, »Special Feature Exhaustive Cryptanalysis of the NBS Data Encryption Standard,« Computer, svez. 10, br. 6, pp. 74 - 84, 1977., doi:10.1109/C-M.1977.217750

[10.] Internet Engineering Task Force (IETF), »Security Architecture for the Internet Protocol,« 12 2005. [Mrežno]. Available: https://datatracker.ietf.org/doc/rfc4301/. [Pokušaj pristupa 27 3 2022].

[11.] Internet Engineering Task Force (IETF), »The Transport Layer Security (TLS) Protocol Version 1.3,« 8 2018. [Mrežno]. Available: https://datatracker.ietf.org/doc/rfc8446/. [Pokušaj pristupa 13. 2. 2022.].

[12.] J. A. Buchmann, Introduction to Cryptography (2nd Edition), New York: Springer, 2004., ISBN: 78-1-4665-7027-6

[13.] T. Kleinjung, K. Aoki, J. Franke I A. K. Lenstra, »Factorization of a 768-Bit RSA Modulus,« u Advances in Cryptology–-CRYPTO 2010, Santa Barbara, 2010., doi:10.1007/978-3-642-14623-7_18

[14.] M. Panda, »Performance analysis of encryption algorithms for security,« u Panda, Madhumita, 2016.

[15.] D. Commey, S. Griffith Klogo i J. Dzisi Gadze, »Performance comparison of 3DES, AES, Blowfish and RSA for Dataset Classification and Encryption in Cloud Data Storage,« International Journal of Computer Applications, svez. 177, br. 40, pp. 17-22, 2020.

[16.] W. Diffie i M. E. Hellman, »New Directions in Cryptography,« IEEE Transactions on Information Theory, svez. 22, br. 6, 11 1976., doi:10.1109/TIT.1976.1055638

[17.] S. Chen, S. Jero, M. Jagielski, A. Boldyreva I C. Nita-Rotaru, »Secure Communication Channel Establishment: TLS 1.3 (over TCP Fast Open) versus QUIC,« Journal of Cryptology, svez. 34, br. 3, 2021., doi:10.1007/978-3-030-2995-0_20

[18.] J. F. Kurose i K. W. Ross, Computer Networking: A Top-Down Approach (8th Edition), Pearson, 2021., ISBN:9780136681557

[19.] Internet Engineering Task Force (IETF), »The Secure Shell (SSH) Protocol Architecture,« 1 2006. [Mrežno]. Available: https://datatracker.ietf.org/doc/rfc4251/. [Pokušaj pristupa 13. 2. 2022.].

[20.] H. Dwivedi, Implementing SSH: Strategies for Optimizing the Secure Shell, Indianapolis: Wiley Publishing, Inc., 2004, pp. 5-12., ISBN: 978-0471458807

[21.] K. Cohn-Gordon, C. D. B. Cremers, L.

Garratt i D. Stebila, »A Formal Security Analysis of the Signal Messaging Protocol,« Journal of Cryptology, br. 33, pp. 1914-1983, 2020., doi:10.1109/EuroSP.2017.27

[22.] Apple Inc., »iMessage security overview,« 18 2 2021. [Mrežno]. Available: https://support.apple.com/en-gb/guide/security/secd9764312f/1/web/1. [Pokušaj pristupa 22 2 2022].

[23.] M. Bellare, A. C. Singh, J. Jaeger, M. Nyayapati, I. Stepanovs, »Ratcheted Encryption and Key Exchange: The Security of Messaging,« u Advances in Cryptology – CRYPTO 2017. CRYPTO 2017. Lecture Notes in Computer Science, vol 10403., 2017., doi:10.1007/978-3-319-63697-9_21

[24.] P. Rösler, C. Mainka i J. Schwenk, »More is Less: On the End-to-End Security of Group Chats in Signal, WhatsApp, and Threema,« u 2018 IEEE European Symposium on Security and Privacy (EuroS&P), 2018., doi:10.1109/EuroSP.2018.00036

[25.] Signal, »Technical information,« [Mrežno]. Available: https://signal.org/docs/. [Pokušaj pristupa 6 3 2022].

[26.] Rakuten Viber, »Viber Encryption Overview,« [Mrežno]. Available: https://www.viber.com/app/uploads/viber-encryption-overview.pdf. [Pokušaj pristupa 6 3 2022].

AUTORI · *AUTHORS*

● **Mirna Pibernik -** Po završetku diplomskog studija Znanstvenog istraživanja masovnih komunikacija upisala je preddiplomski studij Raèunarstva na Tehnièkom veleuèilištu u Zagrebu. Uz studij radi kao razvojni inženjer u tvrtki CROZ.

● **Željko Kovačević -** Viši je predavač na Tehničkom veleučilištu u Zagrebu gdje sudjeluje u nastavi iz kolegija orijentiranih prema učenju programskih jezika i baza podataka. Doktorirao je na Fakultetu elektrotehnike, računarstva i informatike u Mariboru 2022. godine na području razvoja domenski specifičnih programskih jezika. Autor i koautor je 6 knjiga te mnogobrojnih stručnih i znanstvenih radova objavljenih u domaćim i inozemnim časopisima, a 2015.g. dobiva posebno priznanje MVP (Most Valuable Professional) tvrtke Embaracdero za razvoj aplikacija u Embarcadero RAD Studio alatima C++ Builder i Delphi.

Korespondencija · *Correspondence*
zeljko.kovacevic@tvz.hr