Прегледни чланак
343.14:004.424.4
doi:10.5937/zrpfns54-26929

Др Милана М. Писарић, асистент са докторатом
Универзитет у Новом Саду
Правни факултет у Новом Саду
M.Pisaric@pf.uns.ac.rs

ЕНКРИПЦИЈА КАО ПРЕПРЕКА ОТКРИВАЊУ И ДОКАЗИВАЊУ КРИВИЧНИХ ДЕЛА

Сажетак: *Енкрипција је саставни део савременог живота. Она је од несумњивог значаја за остваривање неких од основних људских права у свеприсутном техничком окружењу, за свакодневно коришћење бројних онлајн услуга, као и за функционисање Интернета уопште. С друге стране, органи надлежни за откривање и доказивање кривичних дела се све чешће сусрећу са препрекама када приступе енкриптованим садржајима. Енкрипција представља својеврстан изазов у спровођењу како општих, тако и посебних доказних радњи. Рад је посвећен сагледавању техничких страна овог изазова. Аутор приказује основне принципе на којима се заснива процес енкрипције, објашњава разлику између симетричне и асиметричне енкрипције, енкрипције ускладиштених података и енкрипције података у транзиту, те серверске и корисничке енкрипције, указујући на који начин енкрипција отежава, односно онемогућава рад органа надлежних за откривање и доказивање кривичних дела.*

Кључне речи: *откривање и доказивање кривичних дела, електронски докази, енкрипција.*

1. УВОД

Потреба да се одређени податак и информација садржана у њему прикрију од неовлашћеног лица иманентна је људској природи. Историјски примери криптографије[1] пронађени су у старом Египту, Месопотамији, Кини,

[1] Криптографија је дисциплина која обухвата принципе, средства и методе за трансформисање података, да би се прикрила информација коју податак садржи, утврдила аутентичност података, онемогућила његова неприметна измена и спречио неовлашћен приступ податку. Вид. *OECD Council Recommendation Concerning Guidelines for Cryptography Policy*, C(97)62/FINAL, 27.3.1997, https://www.oecd.org/sti/ieconomy/guidelinesforcryptographypolicy.htm.

а позната је и Цезарова шифра[1] и употреба Енигме током Другог светског рата.[2] Савремена криптографија прати развој технологије рачунарства и комуникационе технологије од 1950-их година, и од тада се криптографске технике развијају и примењују од стране различитих актера. Криптографија као технологија дигиталне безбедности се примењује како би се заштитила безбедност (поверљивост, поузданост и доступност) информација и комуникација, обезбедила анонимност учесника у комуникацији, а тиме и њихова приватност.[3]

Енкрипција, као криптографска технологија дигиталне безбедности,[4] је у 21. веку од несумњивог значаја за остваривање појединих људских права и функционисање дигиталне економије. Енкрипција има за циљ да пружи гаранцију поузданости и целовитости података у информационим системима, а нарочито података о личности, и служи остваривању и заштити свих аспеката права на приватност, слободе изражавања и слободе мишљења и уверења.[5] Она је значајна за заштиту националне безбедности, као и за рад државних органа. Приступ енкрипцији штити од бројних кривичних дела омогућених развојем информационе технологије. Са друге стране, примена енкрипције од стране извршилаца кривичних дела отежава, односно онемогућава рад органа надлежних за откривање и доказивање кривичних дела. Претресање и вештачење рачунара или мобилног телефона ради остваривања приступа похрањеном садржају може да буде отежано, односно онемогућено, уколико је садржај енкриптован.[6] Извршавање тајног надзора комуникације може да буде отежано, односно онемогућено, уколико се комуникација остварује употребом услуга и апликација које примењују енкрипцију.[7] Треба истаћи да се при томе не ради само о енкрипцији коју примењују

---

[1] Више о употреби енкрипције кроз историју, вид. Dwiti Pandya et al., „Brief History of Encryption", *International Journal of Computer Applications* 9/2015, 28-31.

[2] John Barratt, „Enigma and Ultra: the Cypher War", *Military History Online*, http://www.militaryhistoryonline.com/wwii/atlantic/enigma.aspx.

[3] Wolfgang Schulz, Joris van Hoboken, *Human rights and encryption,* Paris 2016, 10.

[4] Технологија енкрипције остварује више функција, јер се користи да би се обезбедила доступност, целовитост, поузданост и/или поверљивост информације садржане у електронском податку који се шифрује. Са становишта предмета овог рада, најзначајнија је функција поверљивости, у смислу да се употребом кључа за енкрипцију садржај података чува као поверљив, односно штити се од приступа неовлашћених лица, јер може да му се приступи само уз познавање кључа за декрипцију.

[5] О значају енкрицпије за промоцију и заштиту приватности, слободе мишљења и изражавања у вези са информационо-комуникационим технологијама, вид. Special Rapporteur of United Nations on the promotion and protection of the right to freedom of opinion and expression, *Research paper on Encryption and Anonymity*, 2018, https://www.ohchr.org/Documents/Issues/Opinion/EncryptionAnonymityFollowUpReport.pdf.

[6] Више о томе, вид. Милана Писарић, *Електронски докази у кривичном поступку*, Нови Сад 2019, 209-210.

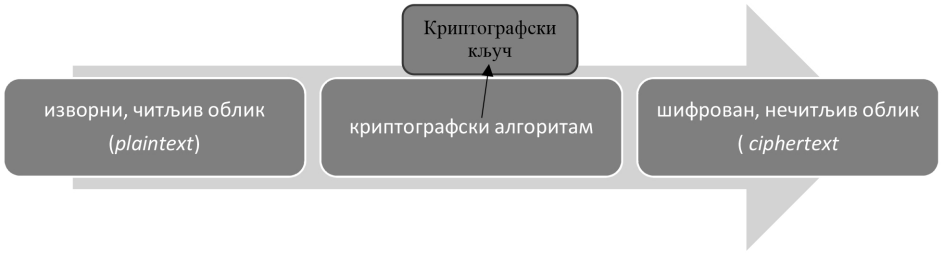
[7] *Ibid*., 218.

технички освешћени и посебно обучени извршиоци. Енкрипција се ургађује као техничка поставка у све већи број уређаја, услуга и апликација, чега корисници нису понекад ни свесни. Постоје бројни софтвери за енкрипцију који се користе, пре свега, у легитимне сврхе, јер омогућавају додатну заштиту података, али исто тако могу да послуже и учиниоцима кривичних дела ради прикривања идентитета и трагова.

2. ШТА ЈЕ ЕНКРИПЦИЈА?

Енкрипција је криптографски процес у ком се податак трансформише из изворног, читљивог облика у шифрован облик, нечитљив за онога ко не поседује знање о механизму примењеном за шифровање, а који је неопходан да се податак дешифрује.

У процесу енкрипције је пет елемената: 1) функција енкрипције, 2) функција декрипције, 3) кључ, 4) текст у изворном облику, и 5) шифровани текст. Ради се о процесу у ком се читљивост података трансформише применом криптографског алгоритма који извршава шифровање. Алгоритам употребом насумичног низа карактера, односно кључа за шифровање (енгл. *key*) претвара податак из изворног, читљивог облика (енгл. *plaintext*) у нечитљиви, шифрован облик (енгл. *ciphertext*). Кључ за енкрипцију састоји се из низа битова, тј. јединица и нула, које рачунар употребом комплексног алгоритма користи да „замаскира“ садржај који се шифрује.



Фигура 1: Упрошћен графички приказ процеса енкрипције

Супротан процес од енкрипције (шифровања) је декрипција (дешифровање), у ком се употребом кључа за дешифровање податак из нечитљивог поново враћа у читљив облик. При томе, енкриптовани садржај може да декриптује само онај ко поседује кључ за декрипцију.

Енкрипција је заправо математичка техника модификовања дигиталног садржаја тако што се у садржају мењају битови (нуле и јединице) применом математичких операција, што га чини неразумљивим. Једини начин да се

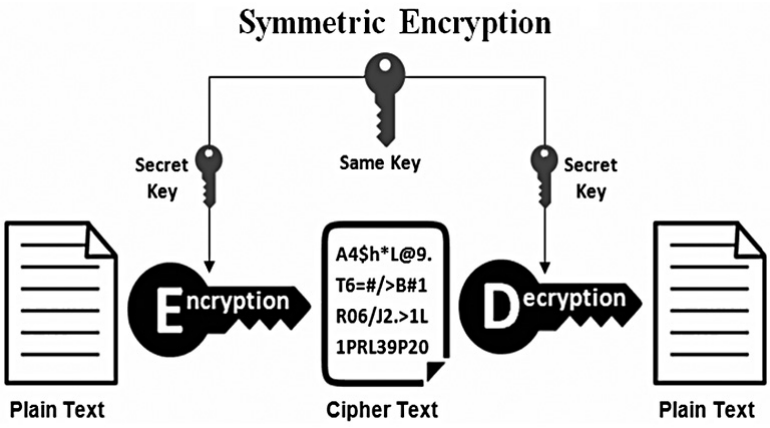
промени шифровани садржај, односно да се врати у оригинални облик, јесте примена обрнуте математичке операције. За сваку операцију шифровања, постоји само једна операција дешифровања, јер су математичке формуле шифровања и дешифровања јединствено повезане и упарене, као брава и кључ за ту браву. Ко не зна или нема приступ математичкој формули за декрипцију, он заправо нема кључ за дешифровање и практично не може да приступи енкрипцијом заштићеним подацима. [8]

Може се разликовати неколико типова енкрипције. У зависноти од тога какав кључ се користи разликују се симетрична и асиметрична енкрипција. У зависности од тога који рачунарски подаци се енкриптују разликује се енкрипција ускладиштених података и енкрипција података у транзиту.

2.1. Симетрична и асиметрична енкрипција

Током времена су се развијали све комплекснији кључеви, а у зависности од тога какав кључ се користи разликују се симетрична и асиметрична енкрипција.

Симетрична енкрипција (енгл. *symmetric encryption*), односно **криптографија приватног кључа** (енгл. *private-key cryptography*) је криптографски процес у ком се један те исти кључ користи и за енкрипцију и за декрипцију.[9]



Фигура 2: Упрошћени графички приказ симетричне енкрипције[10]

[8] Више о томе, вид. Christopher James Hargreaves, Howard Chivers, „Recovery of encryption keys from memory using a linear Scan“, *Proceedings of the 2008 Third International Conference on Availability, Reliability and Security. IEEE Computer Society*, 1369 – 1376, 1374.

[9] Вид. Microsoft, *Description of Symmetric and Asymmetric Encryption*, https://support.microsoft.com/en-us/help/246071/description-of-symmetric-andasymmetric-encryption.

[10] *Encryption: Symmetric and Asymmetric*, https://cryptobook.nakov.com/encryption-symmetric-and-asymmetric.

С обзиром на то да постоји само један кључ, да би податак који је енкриптован могао да се декриптује, неопходно је да лице које остварује приступ податку, односно пошиљалац и прималац података у случају да се енкриптује комуникација, унапред зна који кључ је коришћен.[11] Из тог разлога се стварају одређени стандарди.[12] Од 2001. се као стандард за симетричну енкрипцију података користи *AES* стандард (од енгл. *Advanced Encryption Standard*). *AES* стандард са различитим величинама кључа (од 128, 192 и 256 битова[13]) користи се у већини производа за енкрипцију, протоколима за безбедан пренос података (као што је *HTTPS*, од енгл. *Hypertext Transfer Protocol Secure*), менаџерима за лозинке, појединим апликацијама за слање порука, као и за енкрипцију целог диска уређаја. Осим *AES* стандарда, симетричну енкрипцију користе и други стандардни алгоритми, као што су *Blowfish, Triple DES, Serpent* и *Twofish*.[14]

Асиметрична енкрипција (енгл. *asymmetric encryption*), односно **криптографија јавног кључа** (енгл. *public-key cryptography*) је криптографски

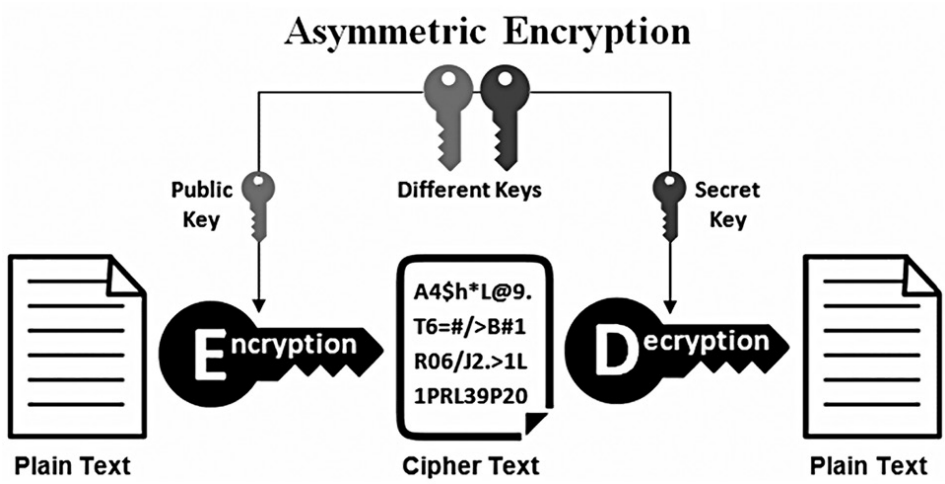
[11] С обзиром на то да се у процесу енкрипције и декрипције користи само један кључ, неопходно је да се чува његова тајност и непредвидљивост његовог „састава“, како би се заштитио од напада, односно од сазанавања од стране неовлашћеног лица. Учесници у комуникацији, тј. пошиљалац и прималац не могу приватну комуникацију да остварују преко јавне рачунарске мреже уколико се претходно не „договоре“ око заједничког, тајног кључа, јер би дистрибуција кључа преко јавне мреже угрозила његову тајност. Због тога је важно да се превазиђу изазови у вези са дистрибуцијом и управљањем кључем – стварањем сигурног комуникацијског канала, путем ког би кључ био познат само онима који имају легитимну потребу за њим (пошиљалац и прималац поруке), и обезбеђивањем великог броја кључева који би били коришћени по потреби.

[12] Након што је од 1960-их дошло до све шире употребе рачунара у комерцијалне сврхе, *IBM* је створио крипто-групу која је током 1970-их имала задатак да дизајнира кључ, са циљем заштите корисникових података. Дизајн настао као резултат рада ове групе, уз учешће Националне службе безбедности САД (енг. *United States National Security Agency* (*NSA*), одабран је 1976. за стандард за енкрипцију података – енгл. *Data Encryption Standard (DES). DES* је био глобални стандард у наредних двадесетак година, али је, након што је 1999. јавно „разбијен“ од стране *distributed.net* и *Electronic Frontier Foundation* (*EFF*), повучен из употребе. Вид. Paul Van De Zande, *The Day DES Died*, https://www.sans.org/reading-room/whitepapers/vpns/daydes-died-722.

[13] Већина криптографских система користи 128-битни или 256-битни симетријски кључ. 128-битни кључ подразумева 2^{128} могућих кључева, односно 340,282,366,920,938,463, 463,374,607,431,768,211,456 комбинација дигита (нумеричких вредности), док 256-битни кључ има могућих 2^{256} кључева, односно дупло више комбинација дигита него 128-битни. (*Cracking Encryption Algorithms*, http://mycrypto.netlencryption/ encryption crack.html). Другим речима, уколико би свако од седам милијарди људи користио десет супер-рачунара од којих би сваки тестирао милијарду комбинација за 128-битни кључ у секунди, било би потребно 77.000.000.000.000.000.000.000.000 година да се „насилно“ пронађе одговарајући кључ за декрипцију. Вид. Mohit Arora, How Secure Is AES Against Brute Force Attacks?“, 5.7.2012, *EE Times*, http://www.eetimes.com/document.asp.

[14] Вид. John Carl Villanueva, „Symmetric vs Asymmetric Encryption“, Jscape, 15.3.2015, https://www.jscape.com/blog/bid/84422/Symmetric-vs-Asymmetric-Encryption.

процес у ком се користе два кључа, један за енкрипцију а други за декрипцију. Ради се о криптографским путем генерисаном пару кључева који су у посебној математичкој корелацији. У оваквом систему један кључ се чува као тајни (приватни кључ) а други је доступан у јавности (јавни кључ) и слободно се дели преко необезбеђене рачунарске мреже. Јавни кључ примаоца поруке се користи да се енкриптује порука која му се шаље, а потом ту шифровану поруку декриптује његов приватни кључ.[15]



Фигура 3: Упрошћени графички приказ асиметричне енкрипције[16]

Асиметрачна декрипција је од значаја за обезбеђивање саобраћаја на Интернету и остваривање електронске комуникације. Постоји више алгоритама који користе асиметричну енкрипцију. Најчешће се користе *RSA* стандард (од енгл. *Rivest-Shamir-Adleman*) и *DSA* стандард (од енгл. *Digital Signature Algorithm*), *ECC* стандард (од енгл. *Elliptic Curve Cryptography*) код мањих уређаја (нпр, мобилних телефона), *OpenPGP* стандард за енкрипцију мејлова, *Signal Protocol* у апликацијама за слање гласовних и видео позива и инстант порука (нпр. као што су Воцап (енгл.*WhatsApp*), Сигнал (енгл. *Signal*) и Фејсбук месинџер (енгл. *Facebook Messanger*).

---

[15] У случају асиметричне енкрипције, пошиљалац и прималац шифрованог податка не морају унапред да се „договоре“ око кључа који ће се користити (као у случају симетричне енкрипције). Корисник А поставља онлајн јавни кључ, која корисник у Б служи да енкриптује поруку упућену кориснику А, а само корисник А може да декриптује поруку шифровану његовим јавним кључем, користећи јединствени тајни, приватни кључ који је у корелацији са јавним кључем.

[16] *Encryption: Symmetric and Asymmetric*, https://cryptobook.nakov.com/encryption-symmetric-and-asymmetric.

2.2. Енкрипција ускладиштених података и енкрипција података у транзиту

Рачунарски подаци могу да буду похрањени у уређају или да се размењују између уређаја, а у зависности од тога који рачунарски подаци се енкриптују, разликује се енкрипција ускладиштених података и енкрипција података у транзиту.

Енкрипција ускладиштених података (енгл. *encryption at rest*) представља процес у ком се шифрују подаци похрањени у уређају за складиштење података (као што су лаптоп, мобилни телефон, сервер пружаоца услуга), чинећи садржај података недоступним за свакога ко не поседује кључ за декрипцију. Корисник употребом посебних софтвера[17] за енкрипцију може да шифрује појединачну датотеку, фолдер, партицију у уређају[18] али и цео диск уређаја.[19] Све је више уређаја (нпр. лаптоп рачунара и мобилних телефона) код којих је енкрипција целог диска (енгл. *full disk encryption*) предвиђена као фабричка поставка (енгл. *by default*) или се уграђују алати за енкрипцију, које корисник може да употреби.[20]

Енкрипција података у транзиту (енгл. *encryption in transit*) представља процес у ком се шифрују подаци који се преносе са једног на други уређај (као што су веб-саобраћај, текстуалне поруке, садржаји који се уносе у веб-формулар и сл.), како би се обезбедили док „путују" од извора до одредишта, односно како би се онемогућило да трећа страна податке пресретне и измени. На тај начин се обезбеђује поверљивост и интегритет садржаја и омогућава његова аутентификација. Енкрипција података у транзиту је од

---

[17] За енкрипцију датотеке и фолдера употребљавају се следећи софтвери: Encrypto, Cryptomator, BoxCryptor, AESCrypt. За енкрипцију целог диска уређаја користе се следећи софтвери: BitLocker, FileVault 2, Linux Unified Key Setup (LUKS), VeraCrypt .

[18] Уколико корисник примени *енкрипцију на нивоу датотеке* (енгл. *file-level encryption*) енкриптује се садржај појединачне датотеке, док посматрач може да уочи њено присуство, као и метаподатке (податак о називу датотеке, када је створена, последњи пут измењена, када јој је последњи пут приступљено, величина датотеке и сл). Поједини алати, као нпр. софтвер *VeraCrypt*, могу да смање видљивост метаподатака.

Осим тога, постоји и технологија која може да маскира присуство енкриптованог драјва у уређају, односно да се применом стеганографске енкрипције диска онемогући да се диск уопште и уочи. Вид. John Leyden, „Russian doll steganography allow users to mask covert drives", The Daily Swig, 10.12. 2018, https://portswigger.net/daily-swig/russian-doll-steganography-allows-users-to-mask-covert-drives.

[19] Енкрипција целог диска подразумева да је енкрипцијом заштићен не само уређај, него и сваки појединачни податак похрањен на хард диску. Другим речима, уколико је диск уређаја у целости енкриптован и уређај искључен, сви садржаји похрањени у њему су шифровани и у потпуности нечитљиви, а покушај да се прикупе подаци из таквог уређаја ће бити неуспешан без кључа за декрипцију.

[20] Нпр. *TrueCrypt software.*

нарочитог значаја за електронске комуникације, а колико је енкрипција сигурна зависи од тога ко има приступ кључу.

Енкрипција на крајњем уређају (енг. *end-to-end encryption: E2EE*) је врста енкрипције података у транзиту у ком се порука енкриптује, односно декриптује у апликацији за пренос података која је инсталирана на уређајима крајњих корисника,[21] тј. учесника у комуникацији. Порука је енкриптована пре него што уђе у комуникацијски канал, као таква чува се на серверу пружаоца услуга док прималац поруке не буде доступан и само уређај примаоца може да је дешифрује, јер само он има приступ кључу за декрипцију. Уколико би трећа страна пресрела поруку у транзиту, не би могла да је декриптује, јер само уређаји крајњих корисника (пошиљаоца и примаоца поруке) имају приступ кључу. Другим речима, пружалац услуга електронске комуникације као посредник у преносу поруке нема могућност да декриптује садржај поруке док се преноси од једног до другог уређаја. Овај вид енкрипције примењен је у апликацијама за пренос порука и обављање разговора, као што су Воцап, Вајр (енгл. *Wire*) и Сигнал. Поруке које се шаљу и разговори који се обављају применом ових апликација су у декриптованом облику доступни једино крајњим корисницима – пружалац телекомуникационих услуга и пружалац услуга елетронских комуникација имају приступ само енкриптованом облику. Поред тога, уколико се користи техника напредне тајности (енгл. *forward secrecy*[22]*) помоћу које се за сваку поруку која се шаље аутоматски генерише јединствени сет кључева за енкрипцију/декрипцију, додатно се компликује могућност дешифровања порука.*

3. КАКО СЕ ПРИМЕЊУЈЕ ЕНКРИПЦИЈА?

Енкрипција се примењује на различитим локацијама, од стране различитих актера. У зависности од тога ко примењује енкрипцију разликују се серверска енкрипција (енгл. *server-side encryption*) и корисничка енкрипција (енгл. *client-side encryption*).[23] **Серверску енкрипцију** примењује трећа страна, односно пружалац услуга, на свом серверу, на податке који за рачун корисника складишти „у облаку“ или преносе кроз рачунарску мрежу. Серверску енкрипцију примењују пружалац онлајн услуга (нпр. мобилно банкарство), пружалац услуга чувања података „у облаку“ (енгл. *cloud service provider*)

[21] Кључеве генерише апликација за слање порука, а не сами корисници.

[22] Jaq Evans, *What is Perfect Forward Secrecy?,* https://www.extrahop.com/company/blog/2017/what-is-perfect-forward-secrecy/.

[23] Linus Chang, „Client-side vs. Server-side encryption – who holds the key?“, *EE News*, 14.5.2018, https://www.eenewseurope.com/design-center/client-side-vs-server-side-encryption-who-holds-key.

и пружалац услуга електронских комуникација. **Корисничку енкрипцију** примењује корисник локално, на податке ускладиштене на свом уређају, на цео уређај или на комуникацију коју остварује са уређаја, коришћењем софтвера и алата за енкрипцију. Безбедност енкриптованих података код серверске енкрипције зависи од пружаоца услуга, јер је он тај који бира врсту, обим и технике енкрипције, док код корисничке енкрипције зависи од уређаја, софтвера и алата које корисник користи, као и од његове свести и техничке оспособљености.

Што се тиче *серверске енкрипције података у транзиту*, да би се од неовлашћеног приступа треће стране заштитио комуникацијски канал између сервера и корисника, многи пружаоци онлајн услуга (услуге електронске управе, електронског пословања и сл.) примењују одређене криптографске технике, активно их интегришући у дизајн и имплементацију услуге коју пружају.[24] Иако примењују енкрипцију у том смислу, пружаоци услуга имају приступ релевантним подацима корисника и могуће је да их предају трећој страни, као што су други комерцијални ентитети или државни органи, вођени финансијским и другим интересима или обавезани прописима.

Многи пружаоци услуга електронских комуникација енкриптују податке у транзиту,[25] али задржавају приступ кључу за декрипцију.[26] *Уколико пружаоци услуга примене одређене криптографске мере ради обезбеђивања повећане приватности корисника (енгл. Privacy Enhancing Technologies:*

---

[24] Примера ради, у платформи за пружање услуге онлајн банкарства примењује се *TLS* стандард за енкрипцију (од енгл. *Transport Layer Security*) који осигурава комуникацију између сервера и клијента банке, гарантујући странама у размени података аутентификацију, тако да клијент може да буде сигуран да су подаци које уноси ради пријављивања у систем (корисничко име и лозинка) доступни само банци.

[25] *TLS* стандард користе и Твитер, Гугл, Џимејл и Јаху, али постоји пружаоци услуга који га не примењују *by default*. Идеално поступање у погледу енкрипције, као вид савршене напредне тајности (енгл. *Perfect Forward Secrecy*), би било да се кључ промени за сваку сесију и да се одбаце коришћени кључеви. Међутим, поједини пружаоци услуга користе исти кључ за енкрипцију дужи временски период. На пример, Фејсбук користи *SSL/TLS* енкрипцију да обезбеди пренос података за пријаву на сајт (енгл. *login*) – када се корисник пријави на страницу, његовом уређају се додељује привремени јединствени идентификатор, помоћу ког се корисник препознаје докле год се не одјави са сервиса.

[26] На пример, у апликацији Телеграм (енгл. *Telegram)* је примењена енкрипција на релацији корисник-сервер/сервер-корисник, али се и поруке које се шаљу чувају на серверу у енкриптованом облику. Међутим, Телеграм има приступ свим кључевима – кључу који енкриптује поруку која се шаље од уређаја пошиљоца до сервера, кључу који енкриптује поруке које се чувају на серверу и кључу који енкриптује поруку која се шаље од сервера до уређаја примаоца поруке. Вид. *Telegram Privacy Policy*, https://telegram.org/privacy.

Слично томе, поруке које се шаљу у Џимејлу јесу енкриптоване и у енкриптованом облику се чувају на серверу чиме су заштићене од приступа неовлашћеног лица, али им Гугл може приступити у изворном облику, јер чува кључеве за декрипцију. Вид. *Google Privacy Policy,* https://policies.google.com/privacy.

PETs), као што је енкрипција на крајњем уређају (енгл. *end-to-end encryption*) [27], њихова способност приступа комуникацијама корисника се ограничава, јер ни пружаоци услуга немају приступ кључу за декрипцију. Ипак, иако пружаоци услуга немају никакву могућност да декриптује податке, метаподаци су видљиви[28] и доступни су му.[29]

Ускладиштени подаци могу да се енкриптују у исто време на више локација. У оквиру тренда да произвођачи уређаја интегришу енкрипцију целог диска у уређаје као фабричку поставку, чиме су енкриптовани сви подаци похрањени у уређају, корисницима се нуди могућност да похрањене податке синхронизују са сервером, односно да их истовремено чувају и „у облаку“ (како би на једном месту били доступни подаци са различитих уређаја, без прекида, нпр. у случају губитка, квара или крађе уређаја). Уколико се корисник енкриптованог мобилног телефона определи да податке похрани и „у облаку“, они се заправо складиште на серверу пружаоца те услуге. У том случају, могућност декрипције података похрањених „у облаку“ зависи од тога који вид енкрипције је пружалац услуге применио.[30]

Од корисникове одлуке о избору уређаја и апликације за комуникацију и начина њиховог коришћења, и о томе где чува податке, да ли се и на који начин подаци енкриптују, зависи и могућност декрипције. Уколико корисник нема поверења у начин на који се подаци „у облаку“ чувају и користе, па податке чува само локално, односно на уређају, могућност декрипције зависи од **софтвера и алата за енкрипцију** које је применио.

---

[27] Пример за технологију повећане приватности је и тзв. систем приватних порука (енгл. *Private messaging*) примењен у апликацијама за размену порука ајмесиџ (енгл. *iMessage*) у ајфон мобилним телефонима.

[28] Тако, иако корисник шаље мејл у апликацији који примењује енкрипцију (нпр. Протонмејл (енгл. *ProtonMail*), подаци у заглављу мејла (предмет, датум и време слања, адреса пошиљаоца и примаоца) неће и не могу да буду енкриптовани јер су неопходно за процес слања поруке. Видљивост метаподатака је оправдана оперативним захтевима. Примера ради, ИП адреса извора и одредишта у комуникацији мора да остане видљива да би мрежна опрема могла да их препозна и очита и тиме омогући пренос података.

[29] Иако Протонмејл енкриптује податке на серверу, метоподаци су видљиви. Вид. ProtonMail, *What is encrypted?*, https://protonmail.com/support/knowledge-base/what-is-encrypted/. Такође, иако Сигнал енкриптује садржај на самом уређају крајњег корисника, али и све податке које складишти и обрађује на свом серверу, може да декриптује одређене податке на серверу (нпр. број телефона регистрованог корисника и податке из његовог профила). Вид. *Signal Terms & Privacy Policy*, https://signal.org/legal/.

[30] Примера ради, уколико се корисник ајфона определи да чува податке „у облаку“ (заправо на *iCloud* серверу), они су енкриптовани, али на њих није примењена *end-to-end* енкрипција, што значи да су доступни, јер Епл чува кључ за декрипцију таквих података. Вид. *iCloud security overview*, Joseph Menn, „Exclusive: Apple dropped plan for encrypting backups after FBI complained – sources“, *Reuters*, 21.1.2020, https://www.reuters.com/article/us-apple-fbi-icloud-exclusive/exclusive-apple-dropped-plan-for-encrypting-backups-after-fbi-complained-sources-idUSKBN1ZK1CT.

Поред поменутих, постоји већи број технологија за повећање приватности у виду софтвера или додатака (енгл. *Browser add-on*) за енкрипцију, који омогућавају поверљивост и тајност комуникација које се остварују на Интернету и анониман приступ онлајн услугама.[31] Постоје алати за анонимизацију који смањују видљивост метаподатака, који омогућавају да се вебсајтовима и онлајн услугама приступи са што мање дигиталних трагова,[32] а нарочито су занимљиви они који се заснивају на енкрипцији, као што су Тор (енгл. *Tor*: *The Onion Router*) и виртуелне приватне мреже (енгл. *VPN*: *Virtual Private Networks*).[33]

Тор је бесплатан *open-source* софтвер[34] који ствара мрежу свих корисника софтвера и омогућава мрежну анонимност тако што маскира изворну

---

[31] На пример, корисник може да инсталира *PGP* софтвер (од енгл. *Pretty Good Privacy*) или *GnuPG* софтвер који енкриптују мејлове док користи услуге Џимејла или другог пружаоца улуга за слање мејлова. Алати као што су *Scramble!* и *Cryptogram* омогућавају *end-to-end* енкрипцију комуникација у друштевним мрежама, а постоје алати који се заснивају на протоколима за *Off-the-Record* (*OTR*) енкрипцију који се примењују у апликацијама за слање инстант порука (нпр. у Фејсбук месинџеру). Вид. *What is off-the-record messaging (OTR)?*, https://www.expressvpn.com/internet-privacy/guides/otr/.

Корисник може додатно да заштити своје податке које шаље на сервер пружаоца услуга тако што садржај претходно енкриптује. Уколико корисник датотеку као прилог (енгл. *attachment*) мејлу пошаље преко Џимејла или је постави на сервер пружаоца услуга за складиштење података у „у облаку“ (нпр. Дропбокс), с обзиром на то да ови пружаоци услуга примењују серверску енкрипцију, могли би да декриптују садржај сачуван на њиховом серверу, јер чувају кључ за декрипцију. Вид. *Dropbox Security*, https://www.dropbox.com/security*, Google Cloud Help – Security*, https://cloud.google.com/security.

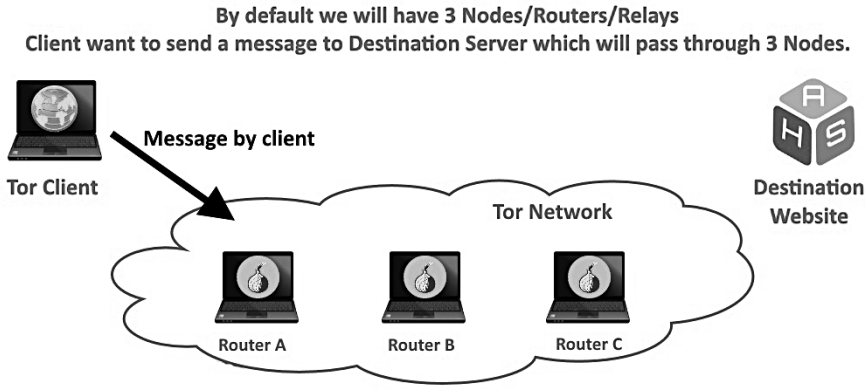
Међутим, уколико је корисник претходно енкриптовао датотеку (нпр. применом *GPG* софтвера за енкрипцију), ови пружаоци услуга не могу да је декриптују јер само крајњи корисник поседује кључ за декрипцију.

[32] Примера ради, као алат за анонимизацију ИП адресе користи се прокси услуга (енгл. *proxy*). Ради се о серверу који посредује у протоку података у саобраћају на Интернету, тако да маскира ИП адресу корисниковог уређаја чинећи да одређена активност изгледа као да се остварује са неке друге локације (нпр. применом протокола *HTTP* и *SOCKS*). Међутим, прокси услуга се не заснива на енкрипцији, па комуникација између корисниковог уређаја и сервера није енкриптована. Осим тога, и уколико се користи протокол *HTTPS* да се прикрије повезаност са одређеним сајтом, не би били видљиви подаци о томе које веб странице је корисник посетио, корисничка имена и лозинке које је унео у веб формуларе и слично, али би његова ИП адреса и други метаподаци и даље били видљиви.

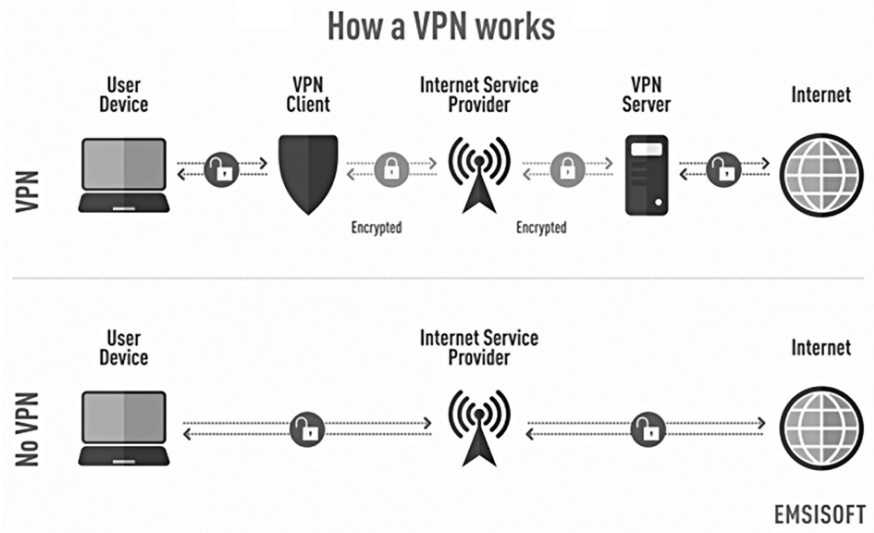
[33] Осим тога, постоје криптографске технологије које прикривају податак у транзиту у оквиру легитимног онлајн садржаја, тј. неког објекта или канала. На пример, технологија *Mobile Magic Mirror* (*M3*) користи технологију која користи уобичајене активности корисника на Твитеру да прикрије неку комуникацију. Вид. Shujun Li, „New information hiding technology to be commercialised by Crossword Cybersecurity“, *Surrey,* 5.3.2016, https://blogs.surrey.ac.uk/sccs/2016/03/05/new-information-hiding-technology-to-be-commercialised-by-crossword-cybersecurity/.

[34] Према подацима од почетка маја 2020. Тор користи преко 2 милиона корисника. Вид. https://metrics.torproject.org/.

ИП адресу корисника кроз неколико (три или више) посредничких, енкриптованих ИП адреса других корисника. Наиме, сваки пут када корисник приступи на Интернет користећи Тор, софтвер аутоматски, позајмљујући неколико ИП адреса за једну такву сесију, ствара насумичну путању састављену од различитих чворова, а сваки чвор је заштићен сопственом слојем енкрипције, која садржи информацију о наредној конекцији.[35]



Фигура 4: Упрошћен приказ конекције преко Тора[36]



Фигура 5: Упрошћен приказ конекције преко виртуелне приватне мреже[37]

[35] Ствара се слојевитост као код лука, отуда *Onion* у називу софтвера.
[36] *How does TOR browser work*?, https://www.quora.com/How-does-TOR-browser-work.
[37] https://www.yellowstonecomputing.net/blog/vpns-your-personal-tunnel-to-privacy-part-2.

Виртуелна приватна мрежа омогућава тајност мрежне комуникације тако да нико не може да пресретне, измени или надзире податке у транзиту. Наиме, уколико корисник инсталира одређени софтвер, његов уређај се повезује са сервером пружаоца ове услуге (енгл. *Remote Access Server*), а применом одређеног протокола[38] ствара се тзв. *VPN* тунел, односно енкриптована веза између уређаја корисника и сервера. Уз помоћ тунела енкриптују се подаци у транзиту (применом асиметричне енкрипције) а и ИП адреса уређаја (тиме и локација корисника) је анонимизирана, јер се користи ИП сервера преко ког је створена виртуелна приватна мрежа.[39]

4. ЕНКРИПЦИЈА КАО ОТЕЖАВАЈУЋИ ФАКТОР ЗА РАД НАДЛЕЖНИХ ОРГАНА

У савременом технолошком окружењу доступност технологије јаке енкрипције довела је до тога да је приступ садржају великог броја електронских података (ускладиштених и у транзиту) отежан, односно онемогућен неовлашћеним лицима, јер не постоји начин да се садржаји енкриптовани модерним алгоритмима декриптују без поседовања кључа за декрипцију. Наиме, садржаји података би, да није енкрипције, били у изворном, читљивом облику доступни надлежним органима приликом спровођења надзора или пресретања комуникације или одузимања и претресања уређаја. У случају да су подаци енкриптовани, њихов садржај је, у моменту када надлежни органи остваре приступ на законом овлашћен начин, доступан само у шифрованом, нечитљивом облику.

Са све масовнијом употребом персоналних рачунара, приступ државних органа енкриптованим подацима постао је предмет озбиљне политичке, научне и стручне дебате. Пре коју деценију било је присутно настојање да се ИТ компаније присиле да „ослабе“ безбедносне протоколе у криптографским системима остављањем могућности „уласка на задња врата“ (енгл. *backdoors*), тј. да угради методе која омогућавају да трећа страна заобиђе те протоколе и оствари приступ енкриптованим садржајима.[40] У првој деценији 21. века постало је јасно да национална ограничења употребе крипто-

[38] Користи се више протокола, као што су *PPTP* (*Point-to-Point Tunneling Protocol*), L2TP (*Layer 2 Tunnel Protocol*), *OpenVPN*, *SSTP* (*Secure Socket Tunneling Protocol*).

[39] Michael Gargiulo, „VPN Encryption: What is it? How does it work?“, *VPN*, 13.12.2019, https://www.vpn.com/privacy/how-does-vpn-encryption-work.

[40] Историјски се може уочити неколико раздобља у којима се води дебата око потребе да се ограничи приступ јакој енкрипцији. Од стварања криптографије јавног кључа, током 1970-их, па до 1990-их држава (првенствено САД) је вршила стриктну контролу над развојем, доступношћу и коришћењем криптографских алата, онемогућавајући широку, комерцијалну употребу јаке енкрипције ван војних и безбедносних оквира.

графије не треба да угрожавају развој информационих и комуникационих мрежа, као ни електронске трговине,[41] што је довело до несметаног процвата технолошког окружења. У овом раздобљу ствара се све више дигиталног садржаја (на друштвеним мрежама, свеприсутни подаци о локацији корисника уређаја, садржаји на онлајн платформама, тј. „у облаку"), а надлежни државни органи добијају читав низ нових техничких могућности и законских овлашћења за прикупљање тих садржаја за потребе кривичног поступка (и заштите националне безбедности). Уколико би се енкрипција појавила као препрека, коришћени су алтернативни начини за прикупљање потребних података.[42] Штавише, не постоје подаци да је у овом периоду енкрипција представљала значајну препреку откривању и доказивању кривичних дела.[43]

Током 1990-их, под притиском приватног сектора и стручне јавности покушало се са стварањем хибридног решења који би истовремено омогућио и развој информационе технологије и нспособност надзирања тог развоја од стране државе. Ова раздобље се назива Првим крипто-ратом. Више о томе, вид. Bruce Schneier, *History of the First Crypto War*, 2015, https://www.schneier.com/blog/archives/2015/06/history_of_the_.html.

Сматрало се да је систем у ком је јавности доступна јака енкрипција неприхватљив јер омогућава да илегалне активности не могу да се прате, па је потребно да јој се ограничи приступ тако што би се установио систем изузетног приступа државних органа кључу за декрипцију. Креиран је стандард депоноване енкрипције (енгл. *Escrowed Encryption Standard: EES*), односно систем депоновања кључа (енгл. *key escrow*), као једноставан метод „уласка на задња врата". Ради се о томе да у криптографском процесу размене кључева копију приватног кључа задржава трећа страна – држава, која ствара и дистрибуира кључеве за енкрипцију ИТ компанијама, а копију кључа за декрипцију држи у депозиту. Креиран је тзв. *Clipper Chip* сет чипова који би био уграђен у уређаје којима би било омогућено да користе *SKIPJACK* алгоритам за енкрипцију. Држава би задржала у депозиту копију тајног кључа, специфичног за чип уграђен у сваки уређај, па би државни органи, по потреби, могли да траже приступ кључевима за декриптовање енкриптованих података. Више о томе, вид. Steven Levy, „Battle of the Clipper Chip", *New York Times*, 12.6.1994, https://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html?pagewanted=all; Michael Schwartzbeck, *The Evolution of US Government Restrictions on Using and Exporting Encryption Technologies*, 2014, https://www.cia.gov/library/readingroom/docs/DOC_0006231614.pdf.

Овај систем је напуштен услед јаког притиска група за заштиту грађанских права и академског концензуса да се на овај начин не обезбеђује тајност комуникација. Истовремено, на снази је била стриктна контрола извоза комерцијалних производа са јаком енкрипцијом из САД, која је либерализована након 1999. Вид. Bill Hancock, „Appeals-court panel says export ban on encryption software is unlawful", *Computers & Security* 4/1999, 278. Више о томе, вид. Kurt Saunders, „The Regulation of the Internet Encryption Technologies: Separating the Wheat from the Chaf", *John Marshall Journal of Information Technology and Privacy Law* 3/1999, 945- 960.

[41] Више о томе, вид. Peter Swire, Kenesa Ahmad, "Encryption and Globalization", *Columbia Science and Technology Law Review* 1/2012, 439-441.

[42] National Security Agency, "Classification Guide Title/Number: Project BULLRUN/2-16", Snowden Archive (16 June 2010), https://snowdenarchive.cjfe.org/ greenstone/collect/snowden1/index/assoc/HASHea20.dir/doc.pdf.

[43] Naomi Gilens, *New Justice Department Documents Show Huge Increase in Warrantless Electronic Surveillance*, ACLU, 2012, https://149 www.aclu.org/blog/national-security/new-justice-

У овом раздобљу, које се назива златно доба надзора (енг. *Golden Age for Surveillance*[44]), *са даљим развојем алата за свеопшти дигитални надзор, надлежни органи су драматично повећали способност за прикупљање до тада невиђене количине електронских података, који се редовно складиште и анализирају*.[45]

Међутим, 2010. ФБИ је указао на проблем „Одласка у мрак" (енгл. *Going Dark*), истакнувши јаз између података којима надлежни органи могу да приступе на законом овлашћен начин и њихове техничке немогућности да остваре увид у садржај тих података.[46] Ради се о томе да, без обзира на то што су сви материјални и формални услови испуњени за приступ електронским подацима, ефикасан приступ информацијама и комуникацијама бива онемогућен енкрипцијом. Наиме, након што је 2013. Едвард Сноуден јавности обелоданио у ком обиму држава спроводи електронски надзор, при чему постоје наговештаји да ИТ компаније пружају помоћ држави у остваривању тог надзора,[47] приметан је тренд да пружаоци Интернет услуга и произвођачи уређаја уграђују енкрипцију као поставку (енгл. *by default*) у својим услугама и уређајима, како би додатно заштитили информације и комуникације корисника и повећали њихово поверење. Тако од 2014. Епл, Гугл и Фејсбук примењују енкрипцију у уређајима и платформама за комуникацију,[48] што ове комапније наводно доводи у положаја да немају приступ корисниковим енкриптованим подацима и због тога не могу да поступе по захтеву државних органа и податке предају за потребе кривичног поступка или заштите националне безбедности. Као последица тога, од 2016. надлежни државни органи непрестано истичу да енкрипција као средство дигиталне

department-documents-show-huge-increase-warrantless-electronic.

[44] Peter Swire, *Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy*, 2015, https://www.hsdl.org/?view&did=794328.

[45] Овакав приступ свеопштем надзору назива се „Прикупи све" (енгл. „*Collect it all*") и доктрина је усвојена у оквиру Америчке службе безедности. Вид. Robert Sloan, Richard Warner, „The Self, the Stasi, the NSA: Privacy, Knowledge, and Complicity in the Surveillance State", *Minnesota Journal of Law, Science & Technology 1/2016*, 373.

[46] Valerie Caproni, *Going Dark: Lawful Electronic Surveillance in the Face of New Technologies*, Federal Bureau of Investigation, prepared testimony for Hearing Before the Subcommittee On Crime, Terrorism, and Homeland Security of the House of Commons Committee on the Judiciary, 2011, http://judiciary.house.gov/hearings/printers/112th/112-59_64581.PDF.

[47] Као на пример, у случају скандала са британском консултантском фирмом Кембриџ Аналитика (енгл. *Cambridge Analytica*). Више о томе, вид. Nicholas Confessore, „Cambridge Analytica and Facebook: The Scandal and the Fallout So Far", *New York Times*, 4.4.2018, https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.

[48] Joe Miller, "Google and Apple to introduce default encryption", BBC, 19.9.2014, https://www.bbc.com/news/technology-29276955; Robert McMillan, „Facebook's WhatsApp Launches 'End-to-End' Encryption", *WSJ*, 5.4.2016, https://www.wsj.com/articles/facebooks-whatsapp-turns-on-encryption-by-default-1459869097.

безбедности све више онемогућава њихов рад на откривању и доказивању тероризма, поседовања и дистрибуирања дечје порнографије и других тешких кривичних дела,[49] а ИТ компаније се оптужују да су створиле „рај за криминалце".[50]

У последњих неколико година предлагано је више решења ради превазилажења проблема енкрипције,[51] тако што би ИТ компанија обавезале да створе могућност „уласка на задња врата",[52] ослабе стандарде енкрипције и омогуће директни приступ у изузетним случајевима, али такви предлози до сада нису озакоњени.[53] Многи од њих су технички неизводљиви или их је немогуће применити на ефикасан начин, јер би се на тај начин угрозила безбедност свих корисника информационе технологије а не само појединачног

[49] Kristin Finklea, *Encryption and the 'Going Dark' Debate*, Congressional Research Service, 2016, https://fas.org/sgp/crs/misc/R44481.pdf.

[50] Igor Bobic, Ryan Reilly, "FBI Director James Comey ‚Very Concerned' About New Apple, Google Privacy Features," *Huffington Post,* 25.9.2014, http://www.huffingtonpost.com/2014/09/25/james-comey-appleencryption_n_5882874.html; Cyrus Vance, "Apple and Google Threaten Public Safety with Default Smartphone Encryption," *The Washington Post*, 26.9.2014, https://www.washingtonpost.com/opinions/apple-and-googlethreaten-public-safety-with-default-smartphone-encryption/2014/09/25/43af9bf0-44ab-11e4-b4371a7368204804_story.html; Charles Hymas, „Facebook is threatening to hinder police by increasing encryption, warns Priti Patel", *Telegraph*, 30.7.2019, https://www.telegraph.co.uk/politics/2019/07/30/facebook-threatening-hinder-police-increasing-encryption-warns/.

[51] Више о томе, вид. Sayako Quinlan, Andi Wilson Thompson, *A Brief History of Law Enforcement Hacking in the United States,* 2016, https://www.newamerica.org/cybersecurity-initiative/policy-papers/brief-history-law-enforcement-hacking-united-states/.

[52] У септембру 2018. коалиција држава „Петоро очију" (енгл. *Five Eyes*), коју чине САД, Канада, Велика Британија, Аутралија и Нови Зеланд, заузела је став да је неопходно да се ИТ компаније принуде да омогуће „улазак на задња врата", чиме би се надлежним органима омогућило спровођење законом прописаних овлашћења и у погледу енкриптованих садржаја. Вид. Lisa Vaas, „Five Eyes nations demand access to encrypted messaging", *Naked security*, 1.8.2019, https://nakedsecurity.sophos.com/2019/08/01/five-eyes-nations-demand-access-to-encrypted-messaging/.

[53] Примера ради, у Аустралији је децембра 2018. усвојен контроверзни Закон о помоћи и приступу телекомуникацијама (енгл. *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*) на основу ког надлежни државни органи могу да упуте ИТ компанијама захтев да им се омогући приступ енкриптованим садржајима, а ове пружају помоћ на добровољној основи. Закон је у току 2019. коришћен у свега седам случајева. Више о томе, вид. Australian Government, Department of Justice, *Telecommunications (Interception and Access) Act 1979 Annual Report 2018–19*, https://parlinfo.aph.gov.au/parlInfo/download/publications/tabledpapers/c424e8ec-ce9a-4dc1-a53e-4047e8dc4797/upload_pdf/TIA%20Act%20Annual%20Report%202018-19%20%7BTabled%7D.pdf;fileType=application%2Fpdf#search=%22publications/tabledpapers/c424e8ec-ce9a-4dc1-a53e-4047e8dc4797%22.

Од почетка 2020. у САД је актуелна дебата око последњег предлога закона (тзв. EARN IT Act) којим би се посредним путем ослабила енкрипција. Више о томе, вид. Zak Doffman, „New Warning Issued For All WhatsApp And iMessage Users: 'Major Threat' To Encryption", *Forbes*, 14.3.2020, https://www.forbes.com/sites/zakdoffman/2020/03/14/new-warning-issued-for-all-whatsapp-and-imessage-users-major-threat-to-encryption/#4d4518153f59.

корисника чијим подацима је потребно приступити у изузетним случајевима, а то би имало бесповратно неповољне последице за сајбер безбедност и електронско пословање. [54] Осим тога, са становишта заштите људских права, енкрипција се сматра средством које служи слободном, отвореном и поузданом Интернету, у оквиру ког је омогућено реализовање гарантованих слобода и права, пре свега права на приватност и слободе мишљења, уверења и изражавања. Из тог разлога, државе се позивају да се суздрже од настојања да обавезују ИТ компаније на примену мера које би ослабиле енкрипцију и тиме компромитовале приватност, те анонимност и безбедност комуникације између корисника њихових услуга.[55]

5. ЗАКЉУЧАК

Неспорно је да је енкрипција од изузетног значаја за заштиту бројних вредности појединца и друштва у целини. Ова технологија сасвим се легитимно користи у циљу заштите тајности, поверљивости и целовитости података, како ускладиштених на уређајима или „у облаку", тако и оних који се преносе у процесу електронске комуникације. Криптографске технологије ће се са појавом нових апликација и уређаја, по свему судећи, развијати и даље, упоредо са све присутнијим импулсима ка свеопштем надзору активности корисника информационих технологија од стране државних органа али и приватних компанија.

Енкрипција служи оправданим интересима појединаца и привредних субјеката, али исто тако и извршиоцима кривичних дела, нарочито за прикривање идентитета и трагова кривичног дела. То за државне органе ствара значајне правне и техничке изазове у откривању и доказивању кривичних дела. Надлежни органи се са изазовима сусрећу када спроводе мере и радње ради прикупљања електронских података за потребе кривичног поступка. Енкрипција целог диска уређаја штити ускладиштене податке од неовлашћеног приступа а енкрипција на крајњем уређају штити податке у транзиту од надзора електронских комуникација. Уколико је примењена енкрипција, надлежни органи остварују приступ подацима у шифрованом, нечитљивом облику који се може превести у изворни, читљиви облик само употребом кључа за декрипцију. Другим речима, енкрипција ускладиштених података

---

[54] Више о томе, вид. Harold Abelson et. al., "Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications", 2015, https://183 www.schneier.com/academic/paperfiles/paper-keys-under-doormats-CSAIL.pdf.

[55] *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, 2015, http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G15/095/85/PDF/G1509585.pdf?OpenElement15.

онемогућава претресање уређаја, док енкрипција података у транзиту онемогућава спровођење тајног надзора и снимања електронских комуникација. У том смислу, овлашћења прописана за спровођење појединих, како општих, тако и посебних доказних радњи, остају само слово на папиру.

С повећаним бројем пружалаца услуга и произвођача који нуде својим корисницима енкрипцију, с једне стране, и вапајем надлежних органа за ограничењем употребе енкрипције и њеним слабљењем отворена је нова рунда у дебати око њене употребе и правног статуса коришћења криптографских технологија уопште. Дебата око енкрипције је комплексна, јер подразумева узимање у обзир више супротстављених интереса (државе, корисника, ИТ компанија) који морају да се узму у обзир, а довођење ових интереса у равнотежу, само по себи, представља изазов за који за сада нема једноставног решења.

Очигледно је да се не одустаје тога да је могуће обавезати криптографе и приватни сектор да пронађу техничко решење и створе такав систем енкрипције у ком би се легитимној страни (држави) омогућио приступ енкриптованим садржајима у изузетним околностима. Иако постоји потреба да се зарад интереса кривичног поступка и заштите националне безбедности створи правни оквир за превазилажење изазова енкрипције, несумњиво је да се при томе морају узети у обзир и дигитална права корисника информационих технологија и интереси ИТ компанија. У научној и стручној јавности је присутно једногласје да тако нешто није могуће без угрожавања принципа на којима модерна енкрипција почива.

Неминовно да ће се државни органи надлежни за откривање и доказивање кривичних дела све више сусретати са изазовима које пред њих поставља ова технологија, стварајући комплексно техничко окружење које се не може разумети без познавања макар принципа на којима се енкрипција темељи. Док се не пронађе адекватно решење комплексних питања у вези са енкрипцијом, овим органима преостаје да јачају своју техничку и тактичку способност, коришћењем дигиталне форензике, и да проналазе алтернативне начине за прикупљање електронских података.

ЛИТЕРАТУРА И ИЗВОРИ

Abelson Harold, et. al., "Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications", 2015, https://183 www.schneier.com/academic/paperfiles/paper-keys-under-doormats-CSAIL.pdf;

AO 442 (Rev. 11/11) Arrest Warrant, Case 2:18mj-00095-BAT, https://regmedia.co.uk/2018/03/13/vincent-ramos-arrest.pdf;

Arora, Mohit, „How Secure Is AES Against Brute Force Attacks?", 5.7.2012, *EE Times*, http://www.eetimes.com/document.asp;

Australian Government, Department of Justice, *Telecommunications (Interception and Access) Act 1979 Annual Report 2018–19*, https://parlinfo.aph.gov.au/parlInfo/download/publications/tabledpapers/c424e8ec-ce9a-4dc1-a53e-4047-e8dc4797/upload_pdf/TIA%20Act%20Annual%20Report%202018-19%20%7BTabled%7D.pdf;fileType=application%2Fpdf#search=%22publications/tabledpapers/c424e8ec-ce9a-4dc1-a53e-4047e8dc4797%22;

Bobic, Igor, Ryan Reilly, "FBI Director James Comey 'Very Concerned' About New Apple, Google Privacy Features," *Huffington Post,* 25.9.2014, http://www.huffingtonpost.com/2014/09/25/james-comey-appleencryption_n_5882874.html;

Chang, Linus, „Client-side vs. Server-side encryption – who holds the key?", *EE News*, 14.5.2018, https://www.eenewseurope.com/design-center/client-side-vs-server-side-encryption-who-holds-key;

Confessore, Nicholas „Cambridge Analytica and Facebook: The Scandal and the Fallout So Far", *New York Times*, 4.4.2018, https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html

Doffman, Zak, „New Warning Issued For All WhatsApp And iMessage Users: 'Major Threat' To Encryption", *Forbes*, 14.3.2020, https://www.forbes.com/sites/zakdoffman/2020/03/14/new-warning-issued-for-all-whatsapp-and-imessage-users-major-threat-to-encryption/#4d4518153f59;

Dropbox Security, https://www.dropbox.com/security;

Dwiti, Pandya et al., „Brief History of Encryption", *International Journal of Computer Applications* 9/2015, 28-31;

Encryption: Symmetric and Asymmetric, https://cryptobook.nakov.com/encryption-symmetric-and-asymmetric;

Evans, Jaq, *What is Perfect Forward Secrecy?,* https://www.extrahop.com/company/blog/2017/what-is-perfect-forward-secrecy/;

Gargiulo, Michael, "VPN Encryption: What is it? How does it work?", *VPN,* 13.12.2019, https://www.vpn.com/privacy/how-does-vpn-encryption-work;

Gill, Lex, Tamir Israel, Christopher Parsons, *Citizen Lab and the Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic: Shining a Light on the Encryption Debate: a Canadian Field Guide*, Toronto 2018;

Google Cloud Help – Security, https://cloud.google.com/security;

Google Privacy Policy, https://policies.google.com/privacy;

Hancock, Bill, „Appeals-court panel says export ban on encryption software is unlawful", *Computers & Security* 4/1999, 278-279;

Hargreaves, Christopher James , Howard Chivers, „Recovery of encryption keys from memory using a linear Scan", *Proceedings of the 2008 Third International Conference on Availability, Reliability and Security. IEEE Computer Society*, 1369 – 1376;

Hoboken, Joris van, *Human rights and encryption,* Paris 2016;

How does TOR browser work?, https://www.quora.com/How-does-TOR-browser-work;

iCloud security overview, https://support.apple.com/en-us/HT202303#:~:text=Data%20security,end%2Dto%2Dend%20encryption;

Hymas, Charles, „Facebook is threatening to hinder police by increasing encryption, warns Priti Patel", *Telegraph*, 30.7.2019, https://www.telegraph.co.uk/politics/2019/07/30/facebook-threatening-hinder-police-increasing-encryption-warns/;

Internet Engineering Task Force*, PKCS #5: Password-Based Key Derivation Function 2 (PBKDF2) Test Vectors*, 2011, https://11 tools.ietf.org/html/rfc6070;
Levy, Steven, „Battle of the Clipper Chip“, *New York Times*, 12.6.1994, https://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html?pagewanted=all;
Leyden, John, „Russian doll steganography allow users to mask covert drives“, *The Daily Swig,* 10.12. 2018, https://portswigger.net/daily-swig/russian-doll-steganography-allows-users-to-mask-covert-drives;
Li, Shujun, *New information hiding technology to be commercialised by Crossword Cybersecurity*, 5.03.2016, https://blogs.surrey.ac.uk/sccs/2016/03/05/new-information-hiding-technology-to-be-commercialised-by-crossword-cybersecurity/;
McMillan, Robert, „Facebook's WhatsApp Launches 'End-to-End' Encryption“, *WSJ*, 5.4.2016, https://www.wsj.com/articles/facebooks-whatsapp-turns-on-encryption-by-default-1459869097;
Menn, Joseph, „Exclusive: Apple dropped plan for encrypting backups after FBI complained – sources“, *Reuters*, 21.1.2020, https://www.reuters.com/article/us-apple-fbi-icloud-exclusive/exclusive-apple-dropped-plan-for-encrypting-backups-after-fbi-complained-sources-idUSKBN1ZK1CT;
Microsoft, *Description of Symmetric and Asymmetric Encryption*, https://support.microsoft.com/en-us/help/246071/description-of-symmetric-andasymmetric-encryption;
Miller, Joe, *"*Google and Apple to introduce default encryption“, *BBC*, 19.9.2014, https://www.bbc.com/news/technology-29276955;
National Institute of Standards and Technology, *Recommendation for Password-Based Key Derivation*, 2010, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-132.pdf;
OECD Council Recommendation Concerning Guidelines for Cryptography Policy, C(97)62/FINAL, 27.3.1997, https://www.oecd.org/sti/ieconomy/guidelinesforcryptographypolicy.htm;
Писарић, Милана, *Електронски докази у кривичном поступку*, Нови Сад 2019;
ProtonMail, *What is encrypted?*, https://protonmail.com/support/knowledge-base/what-is-encrypted/;
Quinlan, Sayako Andi Wilson Thompson, *A Brief History of Law Enforcement Hacking in the United States,* 2016, https://www.newamerica.org/cybersecurity-initiative/policy-papers/brief-history-law-enforcement-hacking-united-states/;
Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 2015, http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G15/095/85/PDF/G1509585.pdf?OpenElement15;
Saunders, Kurt, „The Regulation of the Internet Encryption Technologies: Separating the Wheat from the Chaf“, *John Marshall Journal of Information Technology and Privacy Law* 3/1999, 945- 960;
Schneier, Bruce, *History of the First Crypto War*, 2015, https://www.schneier.com/blog/archives/2015/06/history_of_the_.html;
Schneier, Bruce, *Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C (cloth)*, Indianapolis 2015;
Schwartzbeck, Michael, *The Evolution of US Government Restrictions on Using and Exporting Encryption Technologies*, 2014, https://www.cia.gov/library/readingroom/docs/DOC_0006231614.pdf;

Signal Terms & Privacy Policy, https://signal.org/legal;
Sloan, Robert, Richard Warner, „The Self, the Stasi, the NSA: Privacy, Knowledge, and Complicity in the Surveillance State“, *Minnesota Journal of Law, Science & Technology 1/2016,* 347-408;
Special Rapporteur of United Nations on the promotion and protection of the right to freedom of opinion and expression, *Research paper on Encryption and Anonymity*, 2018, https://www.ohchr.org/Documents/Issues/Opinion/Encryption-AnonymityFollowUpReport.pdf;
Swire, Peter, Kenesa Ahmad, "Encryption and Globalization", *Columbia Science and Technology Law Review* 1/2012, 416-481;
Swire, Peter, *Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy*, 2015, https://www.hsdl.org/?view&did=794328;
Telegram Privacy Policy, https://telegram.org/privacy;
Van De Zande, Paul, *The Day DES Died*, https://www.sans.org/reading-room/white-papers/vpns/daydes-died-722;
Vaas, Lisa, „Five Eyes nations demand access to encrypted messaging“, *Naked security*, 1.8.2019, https://nakedsecurity.sophos.com/2019/08/01/five-eyes-nations-demand-access-to-encrypted-messaging/;
Vance, Cyrus, "Apple and Google Threaten Public Safety with Default Smartphone Encryption," *The Washington Post*, 26.9.2014, https://www.washingtonpost.com/opinions/apple-and-googlethreaten-public-safety-with-default-smartphone-encryption/2014/09/25/43af9bf0-44ab-11e4-b4371a7368204804_story.html;
Villanueva, John Carl, *Symmetric vs Asymmetric Encryption, Jscape,* 15.3.2015, https://www.jscape.com/blog/bid/84422/Symmetric-vs-Asymmetric-Encryption;
What is off-the-record messaging (OTR)?, https://www.expressvpn.com/internet-privacy/guides/otr/.

Milana M. Pisarić, Assistant with Ph.D.
University of Novi Sad
Faculty of Law Novi Sad
M.Pisaric@pf.uns.ac.rs

Encryption as an Obstacle for Crimimanl Investigation and Evidence Collection

Abstract: *Encryption has become an integral part of modern life. It is without a doubt of great importance for the realization of some of the basic human rights in the ubiquitous technical environment, for the daily use of numerous online services, as well as for the functioning of the Internet in general. On the other hand, the authorities in charge of detecting and proving crime are increasingly facing obstacles when accessing encrypted content. Namely, encryption represents a kind of challenge in the implementation of both general and special evidentiary actions. This paper is dedicated to understanding the technical aspects of this challenge. The author explains the basic principles on which encryption technology is based, pointing out the difference between symmetric and asymmetric encryption, between encryption of stored data and data encryption in transit, and between server-based and user-based encryption, and its implication for investigation of crime.*

Keywords: *criminal investigation, electronic evidence, encryption.*

Датум пријема рада: 05.06.2020.