TOR
OMEMO
OTR GPG

Kriptoparti priručnik

CRYPTO PARTY

Cryptoparty rečnik

Model pretnje (eng. *Threat model*) je sistem ili model za određivanje nivoa potrebne sigurnosti na osnovu pretpostavljenih sposobnosti napadača.

Tekst ili poruka (eng. *Plaintext*) je nešifrovana, nezaštićena poruka ili tekst razumljiv čoveku.

Šifrat (eng. *Ciphertext*) je šifrovana poruka ili informacija nerazumljiva čoveku za koju je potreban ključ ili šifra kako bi se razumela.

OTR (eng. *Off-The-Record*) je protokol (skup pravila) za šifrovanu i verifikovanu čet komunikaciju dva korisnika.

OMEMO (eng. OMEMO Multi-End Message and Object Encryption) je protokol koji omogućava šifrovano dopisivanje više korisnika sa više uređaja, uglavnom preko XMPP mreže.

Otisak (eng. *Fingerprint*) je kratak i jedinstveni niz karaktera matematički vezan za veći ključ za šifrovanje – obično javni ključ. Koristi se za proveru da koristite odgovarajući javni ključ osobe sa kojom šifrovano komunicirate.

Internet provajder (eng. *Internet Service Provider* – ISP) je pružaoc usluge pristupanja internetu.

XMPP (Exstensible Messaging and Presence Protocol) je protokol za razmenu trenutnih poruka.

Cryptoparty rečnik

PGP (*Pretty good privacy*) je jedan od prvih kriptografskih softvera za šifrovanje dostupan civilnim licima devedesetih godina.

OpenPGP je otvoreni protokol i standard za softver koji obavlja šifrovanje poruka.

GPG (*Gnu Privacy Guard*) je implementacija OpenPGP standarda pod *GPL* licencom od strane fondacije slobodnog softvera (*FSF*) .

Javni ključ (eng. *Public key*) je deo para asimetričnih ključeva koji neko koristi kada treba da šifruje poruku koju ćete samo vi moći da dešifrujete i odgovara vašem tajnom ključu.

Tajni ključ (eng. *Private key*) je drugi, tajni deo asimetričnog para ključeva koji ne delite sa drugima, služi da dešifrujete šifrovane poruke poslate vama, kao i za digitalno potpisivanje.

SSL *(Secure Socket Layer)* je način obezbeđivanja komunikacije između vašeg računara i veb sajta na koji se povezujete.

IM (Instant messaging) je brzo dopisivanje u realnom vremenu kada su učesnici konverzacije u isto vreme na mreži.

Izvor: **https://goo.gl/ivG521** i Vikipedija

Šifrovanje elektronske pošte

Tunderbird (eng. Thunderbird) je mejl klient za desktop operativne sisteme koji zajedno sa Enigmejl (eng. Enigmail) dodatkom ima mogućnost šifrovanja, dešifrovanja, digitalnog potpisivanja i provere digitalnih potpisa elektronskih poruka.
Podržane platforme: Windows, Mac, Linux.

mozilla.org/thunderbird/

K-9 Mejl (eng. K-9 Mail) je mejl klijent otvorenog koda za android mobilne telefone. Zajedno sa gpg menadžerom kao što je APG ili OpenKiČejn (eng. OpenKeyChain) može šifrovati, dešifrovati, digitalno potpisivati i proveravati digitalno potpisane poruke.
Podržane platforme: Andoid.

k9mail.github.io/download.html

Više na: https://www.privacytools.io/#clients

Enigmejl (eng. *Enigmail*) je dodatak za Tanderbrd (eng. *Thunderbird*) mejl klijenta i GPG menadžer koji vam omogućava da lako šifrujete, dešifrujete, digitalno potpisujete poruke i proveravate digitalne potpise primljenih poruka.

enigmail.net/index.php/en/
mozilla.org/en-US/thunderbird/

GPG tuls (eng. *GPG Tools*) je program za Mek operativni sistem (eng. *Mac OS*) i menadžer ključeva koji omogućava da lako šifrujete, dešifrujete, digitalno potpisujete poruke i proveravate digitalne potpise primljenih poruka. Radi sa preinstaliranim mejl klijentom na Mek sistemu.

gpgtools.org

APG (*Android Privacy Guard*) je OpenPGP implementacija za Android i menadžer ključeva koja omogućava šifrovanje, dešifrovanje, digitalno potrpisivanje I proveru digitalnih potpisa primljenih poruka. Radi u kombinaciji sa mejl klijentom kao što je K-9.

Više na: https://www.privacytools.io/#clients

OpenKiČejn (eng. OpenKeyChain) je GPG menadžer za android operativne sisteme. Radi šifrovanje, dešifrovanje, digitalno potpisivanje i proveru digitalno potpisanih poruka pri nekom mejl klijenti kao što je K-9.
Podržane platforme: Android

openkeychain.org

Kibejs (eng. Keybase) je platorma za šifrovano dopisivanje, deljenje fajlova i služi kao registar javnih ključeva.
Podržane platforme: Windows, Linux, Mac, Android, iOS, Chromium/Firefox

keybase.io

p≡p

PEP (pretty Easy privacy) je aplikacija za šifrovanje mejlova koja eliminiše potrbu za serverima javnih ključeva, šaljući iste uz mejl poruke, ali zahteva da korisnici jedni druge verifikuju (uživo, ili putem drugog kanala komunikacije).
Podržane platforme: Android

prettyeasyprivacy.com

Mejlvelop (eng. Mailvelope) je dodatak za Hrom i Fajrfoks internet pregledače koji omogućava šifrovanje tektualnih poruka iz pregledača na sajtovima GMX, Yahoo, Gmail I Outlook.

mailvelope.com

Zaštita na mreži

Tor mreža je grupa volonterskih servera koji omogućava ljudima da poboljšaju svoju privatnost i sigurnost na Internetu i zaobiđu cenzuru. Tor omogućava korisnicima da razmjenjuju informacije preko javnih mreža bez ugrožavanja njihove privatnosti.
Podržane platforme: Windows, Mac, Linux, iOS, Android, OpenBSD

torproject.org

Tor pretraživač je modifikovana verzija Mozilinog Fajerfoks pretraživača koji svu komunikaciju štiti upotrebom Tor anonimne mreže. Dolazi sa već instaliranim dodacima za povećanje privatnosti. Port 9150.
Otvorenog je koda, a podržane platforme su: Windows, Mac, Linux, iOS, Android, OpenBSD.

torproject.org

Orbot je Tor softver za android mobilne telefone koji se povezuje na Tor mrežu I vašem sistemu i aplikacijama pruža pristup ka Tor mreži kroz port 8118.
Podržane platforme: Android.

guardianproject.info/apps/orbot/

Šifrovano dopisisvanje

Gajim je je multiplatformski klijent za dopisivanje. Nudi šifrovanje poruka između klijenta i servera, i između dva klijenta korišćenjem OTR i/ili OMEMO dodatka.
Podržane platorme: Windows, Linux, BSD.

gajim.org

Pidžin (eng. Pidgin) je multiplatformski klijent za dopisivanje. Nudi šifrovanje poruka između klijenta i servera, i između dva klijenta korišćenjem OTR i/ili OMEMO dodatka.
Podržane platforme su: Windows, Linux, Mac, BSD.

pidgin.im

Adium je klijent za dopisivanje za Mac operativne sisteme, koji podržava OTR šifrovanje poruka i autentifikaciju između dva klijenta. Za Adium postoji I OMEMO dodatak, ali se za sada mora kompajlirati.

adium.im

Koj (eng. Coy) je multiplatformski klijent za brzo dopisivanje putem XMPP protokola sa ugrađenom podrškom za OTR.
Podržane platforme: Windows, Mac, Linux

coy.im

Konverzejšn (eng. Conversation) je klijent za brzo dopisivanje na android telefonima koji ima ugrađenu podršku za OTR i OMEMO šifrovanje.
Podržane platforme: Android

conversations.im
f-droid.org/en/packages/eu.siacs.conversations/

Čet-sekjur (eng. ChatSecure) je program za mobilne telefone koji šifruje dopisivanje preko interneta upotrebom XMPP protokola. Podržava OTR I OMEMO šifrovanje.
Podržane platforme: iOS

chatsecure.org

Ksaber (eng. Xabber) je XMPP klijent za Android koji ima ugrađenu podršku za OTR.
Podržane platforme: Android, web.

xabber.com

Zom je XMPP klijent za mobilne uređaje koji ima ugrađenu podršku za šifrovanje poruka putem OTR I OMEMO protokola. Veoma lak za korišćenje, korisnik uopšte ne podešava ključeve za šifrovanje, sve je automatizovano i radi u pozadini.

zom.im

Uputstva:

Mejl šifrovanje:

- **Windows: https://cryptoparty.rs/gpgWin.html**
- **Linuks: https://cryptoparty.rs/gpgLin.html**
- **Mac OS X: https://cryptoparty.rs/gpgMac.html**
- **Android: https://cryptoparty.rs/gpgAnd.html**

Šifrovanje brzog dopisivanja (IM):

- **Windows: https://cryptoparty.rs/OtrAnd.html**
- **Linuks: https://cryptoparty.rs/OtrAnd.html**
- **Mac OS X: https://cryptoparty.rs/OtrMac.html**
- **Android: https://cryptoparty.rs/OtrAnd.html**

PGP serveri javnih ključeva:

- **http://pgp.mit.edu**
- **http://pgp.key-server.io**

XMPP javni serveri:

- **xmpp.is**
- **core.mx**

više na: xmpp.net/directory.php

Dodatno:

Šifrovanje pomoću **GPG-**a nije ograničeno samo na mejlove, već se može primenjivati i na forumima i društvenim mrežama, blogovima itd. radi privatnosti i/ili autentičnosti poruka.
Takođe **GPG** služi i za šifrovanje i digitalno potpisivanje fajlova.
Do nedavno je bio aktivan dodatak pod nazivom **WebPG** za veb pregledače koji je nudio **GPG** funkionalnost na veb stranama:

https://webpg.org/

Takođe postoji i onlajn servis sa kojim iz veb pregledača šifrovati mejl sa javnim ključem željenog sagovornika:

https://encrypt.to/

Postoji još jedan program pod nazivom **Autocrypt** koji pokušava da developere upozna sa šifrovanjem mejlova i time doprinese bolje i lakše iskustvo pri upotrebi šifrovanja kod krajnih korisnika:

https://autocrypt.org/

Omemo je u zadnje vreme sve zastupljeniji i polako zamenjuje **OTR**, a koliko tačno je zastupljen možete ispratiti na:

https://omemo.top/

Što se **OTR** protokola tiče postoji, iako malo zastareo, sajt sa više informacija:

https://www.otr.im/

Korisni linkovi:

https://www.privacytools.
https://www.eff.org/node/82654
https://prism-break.org/en/
https://ssd.eff.org/en
https://myshadow.org/
https://securityinabox.org/en/
https://freedom.press/training/
https://pack.resetthenet.org/
https://cryptoparty.rs/