

cryptography: our key to privacy and security

October, 2022
for Global Encryption Day

Strong encryption is a fundamental part of how we remain safe online and offline. It means people can communicate with another person safe in the knowledge no-one is listening in or tampering with their messages.

Despite this, governments around the world are ramping up their attacks on end-to-end encryption (E2EE). Governments view it as a hurdle for law enforcement agencies. But systematically weakening people's digital safety is not the answer.

End-to-end encryption is the gold standard of security in a world where daily life is increasingly online. We need to push back against government efforts to undermine E2EE.

On Global Encryption Day, we need you to join our efforts to protect end-to-end encryption and defeat any proposals that undermine it. We've already shown how attempts to create backdoors in end-to-end encryption are untenable. Now we need to stop the other shortcuts that governments are suggesting.

Source: <https://www.globalencryption.org/2022/06/global-encryption-day-2022/>

Global Encryption Coalition and Global Encryption Day

Global Encryption Coalition:

- established 2020.
- currently has about 300 member organisations/individuals.
- website: <https://www.globalencryption.org/>



Global Encryption Day:

- aim: to **promote and defend strong encryption** as being critical for for our safety (privacy and security).
- when: October 21st(Fri), 2022; annually since 2020.
- events listing:
<https://www.globalencryption.org/events/ged/2022-events/>

what is encryption?

cryptography:

- "crypto" (hidden, secret) + "graphy" (art, science).
- the study and practice of **secure communication** in an adversarial environment.
- includes encryption but also signing, hashing, anonymisation, ...
- underlying mechanisms: mathematics, computer science, code.

encryption:

- the process of **making information unreadable**.
 - opposite term: decryption.
- "encryption" may also mean cryptography in general.

from now on, will refer to it as "cryptography".

background of encryption

Cold War era:

- encryption classed as a "munition" and export controlled.

Crypto Wars (1990s):

- PGP (cryptosystem) released 1991, export from US as a book (1995).
- Clipper Chip (backdoor) made by NSA in 1993, defunct by 1996.

Snowden revelations (2013):

- BULLRUN (NSA encryption weakening program) was revealed.
- triggered more adoption, review and hardening of encryption.

Crypto Wars 2 (2014–present):

- Apple and Google removed their access to encrypted data on phones (2014), US gov. condemnation; Apple–FBI dispute (2016).
- legislative threats: UK Investigatory Powers Act (2016), AU Assistance and Access Act (2018), US EARN IT Bill (2020–present), ...

current and emerging threats against encryption

punitive measures against encryption users:

- coerced key/password disclosure or decryption.
- encryption import/export/use regulations.
- lawful and unlawful hacking of people's devices.
- device searches by police and at border crossings.

technical obstacles:

- web servers denying service to VPN/Tor users.
- blocking of websites that provide privacy tools.
- widespread internet censorship and shutdowns.

other:

- disinformation/propaganda blaming encryption for terrorism, extremism, organised crime, child exploitation, ...
- legislative bills: ChatControl (EU), EARN IT Bill (US), LEAD Bill (US), ...

modern society's adversarial environment

- internet surveillance is routinely committed by various actors.
- cameras, smartphones and other sensors are rampant.
- every aspect of our lives is being intensely digitised.
- many actions and interactions are permanently recorded.
- laws and norms change over time; records pose a growing threat.
- algorithms are replacing human judgement.
- our data is being abused arbitrarily for stalking, profit, etc.
- phishing and cyberattacks are increasing; enabled by past data breaches, digitisation and negligent security practices.
- peaceful protests, human rights defenders, journalists and whistleblowers are frequently targeted by violent institutions.
- authoritarian measures are infiltrating "liberal democracies".

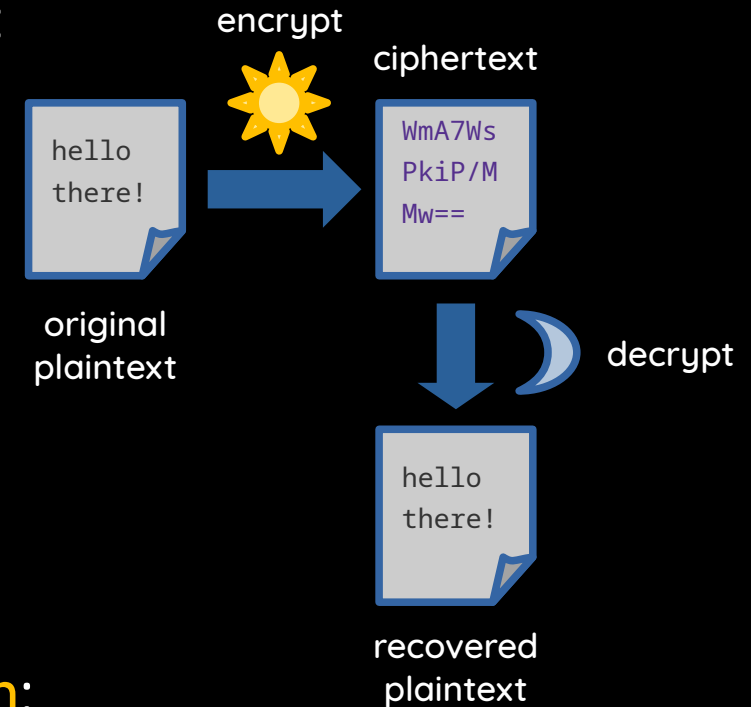
the importance of cryptography

- in modern society, cryptography **helps protect us and society** from surveillance, and secure our digital systems.
- we can use cryptography as a **non-violent technological tool** to enforce confidentiality, anonymity, integrity and authenticity.
- from individuals to communities and societies, **cryptography is vital** for business, democracy, freedom, privacy, safety and trust.
- example uses: social support, legal confidentiality, family matters, love relationships, medical confidentiality, direct action, business.

basic concepts (1) — encryption

symmetric key a.k.a. secret key encryption:

- encrypt and decrypt data with the same secret/common key.
- the encryption and decryption mechanisms are fast.
- securely sharing the secret key/password is problematic.



asymmetric key a.k.a. public key encryption:

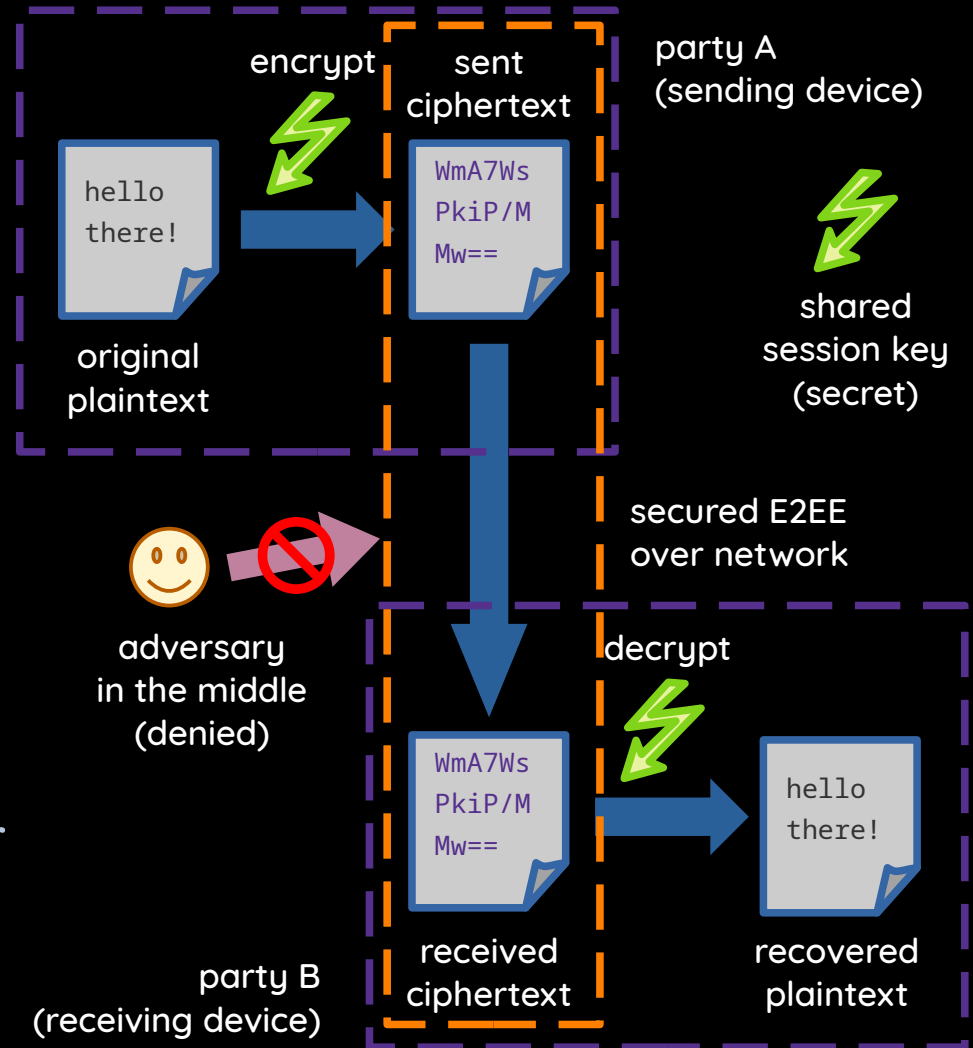
- encrypt with public key; decrypt with private key.
- the public key is safe to publish, easy to share.



basic concepts (2) — end-to-end encryption

end-to-end encryption (E2EE):

- most often combines asymmetric and symmetric key encryption.
- usually involves some form of authenticating the parties.
- each party has sole control over their own private keys.
- no non-party keys are involved.
- no intermediary can eavesdrop or manipulate the communication.



basic concepts (3) — anonymity

anonymity:

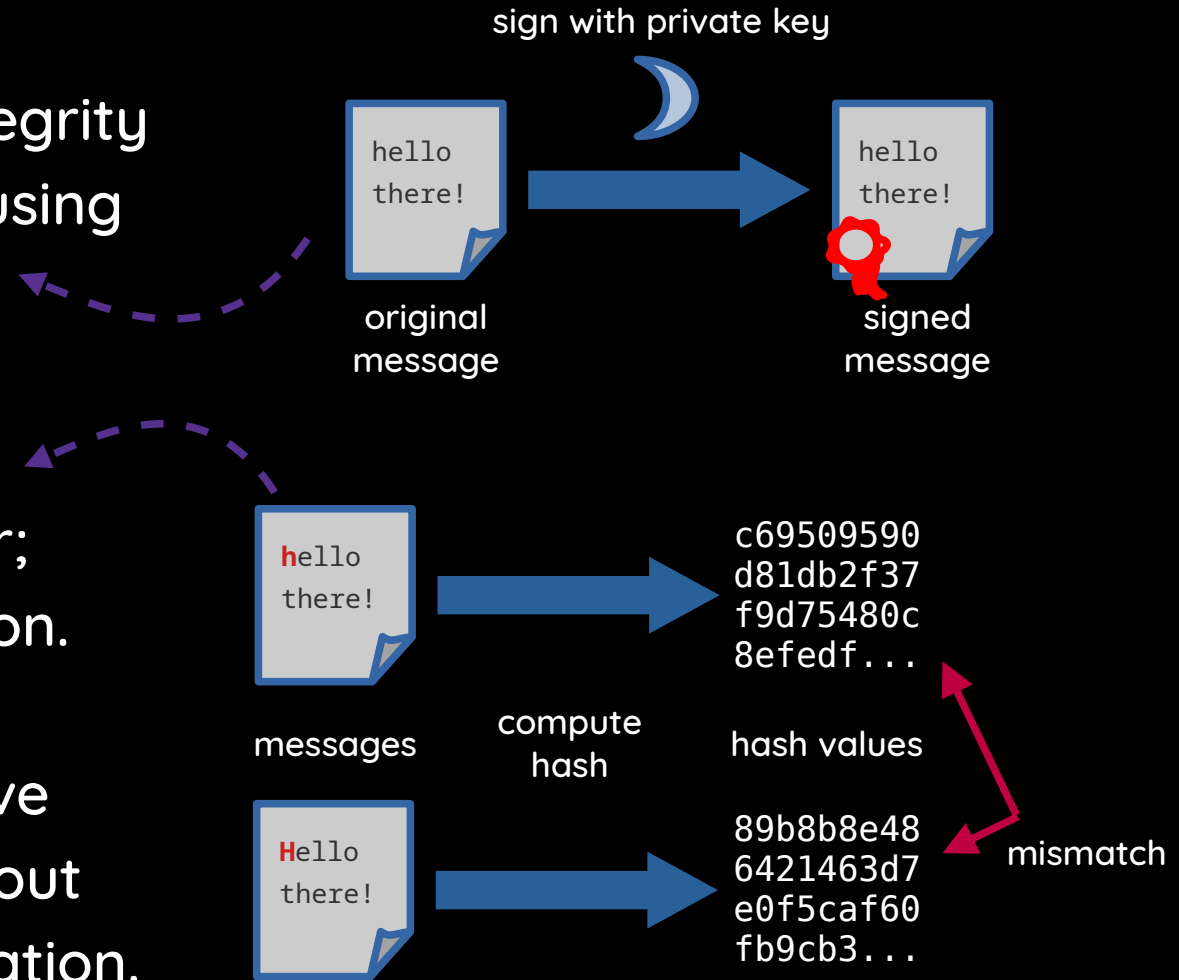
- the state of not being identifiable.
- contrasts with encryption that protects confidential information.
- anonymisation examples:
 - create no identifying information.
 - conceal the origin and destination of internet traffic.

pseudonymity:

- use of a name that is not tied to one's real identity.
- weaker protection than anonymity; one's activities can be linked.
- in contrast to anonymity, allows easy building of reputation.

basic concepts (4) — not just encryption

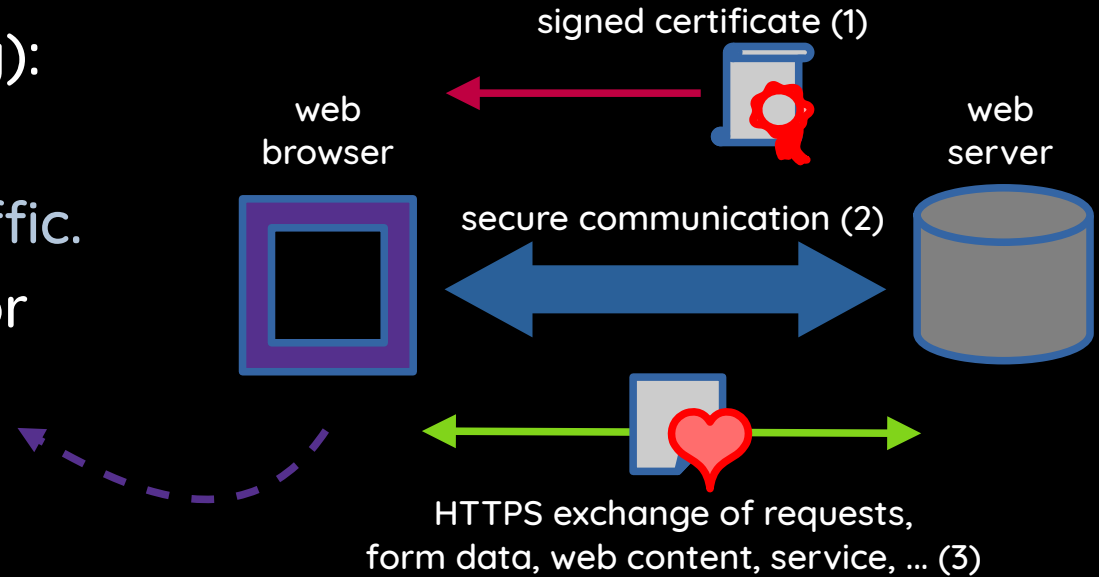
- **signing**: create proof of integrity and authenticity for data, using a private key.
- **hashing**: deterministically convert data into a number; used for integrity verification.
- **zero-knowledge proof**: prove that something is true without disclosing anymore information.



applications (1) — network traffic encryption

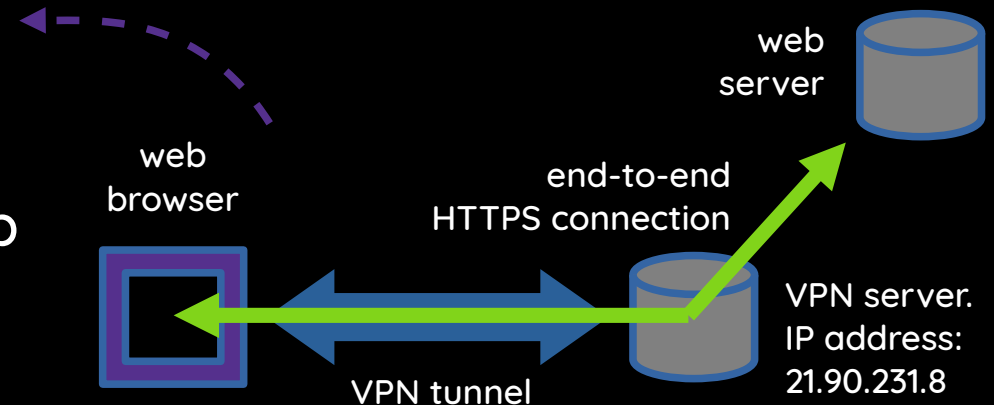
TLS (transport layer security):

- applicable to: mail, web (HTTPS), various other traffic.
- certificates (public keys) for server authentication and common key exchange.



VPN (virtual private network):

- creates secure tunnels between separate networks.
- often used to bypass censorship and weakly protect user IP address.



applications (2) — network traffic anonymisation

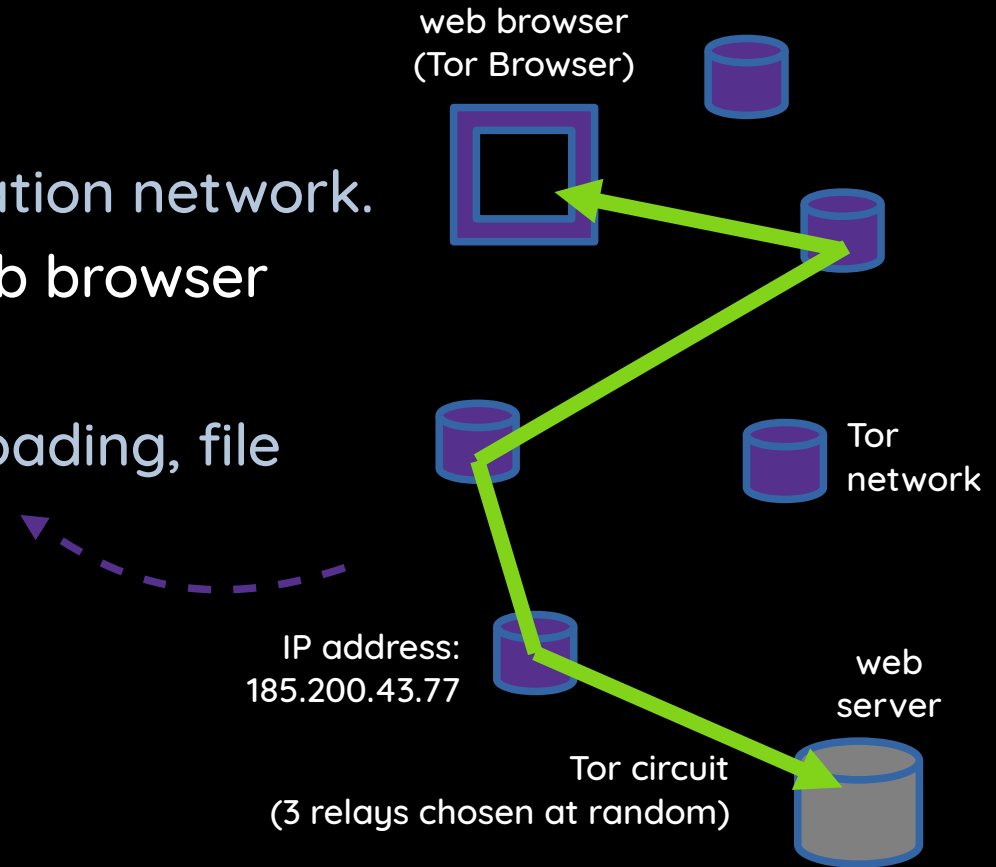
use the internet (more) anonymously.

Tor: <https://torproject.org/>

- the most widely used anonymisation network.
- Tor Browser: a Firefox-based web browser specialised for anonymity.
- use cases: web browsing, downloading, file sharing, messaging, ...

other networks:

- **I2P** : <https://geti2p.net/>
- **Lokinet** : <https://lokinet.org/>
- **Nym** : <https://nymtech.net/>



applications (3) — E2EE secure communication

- **Briar** resilient peer-to-peer messaging: <https://briarproject.org/>
- **Cwtch** Tor-based decentralised messaging: <https://cwtch.im/>
- **Jami** SIP-based peer-to-peer messaging: <https://jami.net/>
- **Jitsi** video chat: <https://jitsi.org/>  **E2EE only in peer-to-peer mode**
- **OnionShare** file sharing and web hosting: <https://onionshare.org/>
- **OpenPGP** file/data and email cryptography: <https://openpgp.org/>
- **Session** decentralised messaging: <https://getsession.org/>
- **SSH** for connecting to shell on remote machines.
- **Signal** centralised messaging: <https://signal.org/>  **phone number**

applications (4) — other cryptography

encryption at rest:

- Android and iOS full-device encryption.
- **KeePassXC** PC password manager: <https://keepassxc.org/>
- **KeePassDX** Android password manager: <https://keepassdx.com/>
- **LUKS** filesystem encryption.
- **VeraCrypt** encrypted filesystem: <https://www.veracrypt.fr/en/>

signing and verification:

- **OpenPGP** file/data and email cryptography: <https://openpgp.org/>

hash computation:

- **shasum, sha512sum, b2sum, etc.** available in BSD, Cygwin, GNU/Linux, macOS and Termux.
- **GtkHash** GUI tool: <https://gtkhash.org/>
- **OpenSSL** command line tool: <https://www.openssl.org/>

best practices when using cryptography (1)

general:

- use strong random passwords generated from good randomness.
- check your area's legal/political context about cryptography use.
- ensure encryption is enabled in software that doesn't enforce it.
- secure your devices from unauthorised access and malware.

cryptography security:

- use proven crypto libraries/applications, securely configured.
- reject vulnerable and potentially compromised algorithms/modes:
 - elliptic curve cryptography: brainpool, NIST, secp256k1, ...
 - symmetric key encryption: 3DES, RC4, XOR cipher, ...
 - random number generation: Dual_EC_DRBG.

best practices when using cryptography (2)

keys:

- authenticate your contacts before trusting the communication.
- don't disclose your private keys to anyone.
- if you suspect your keys are compromised, transition to new private keys and inform your contacts of it.

software:

- use proven free and open-source software (FOSS).
- check features, usability, requirements, development status and appropriateness before adopting software.
- download, verify and regularly update software securely from official sources.

call to action

cultural:

- **normalise** privacy, anonymity, consent and information security.
- **encourage cryptography use** in your groups and communities.

political:

- **reject and counter** propaganda/policies that are pro-surveillance, anti-privacy, anti-anonymity or anti-encryption.
- emphasise **cryptography empowers us** and protects society.

technical:

- **use cryptography** as often and widely as possible.
- **support** FOSS cryptography projects via donations, code, testing/reporting, localisation, documentation and service hosting.

links and resources

Global Encryption Coalition

<https://www.globalencryption.org/>

videos: <https://www.youtube.com/channel/UCMh32OaTNU2P5CtOk0l8V8Q>

Global Encryption Day 2022 events

<https://www.globalencryption.org/events/ged/2022-events/>

Electronic Frontier Foundation, Surveillance Self-Defense

<https://ssd.eff.org/>

Eric Hughes (1993), *A Cypherpunk's Manifesto*

<https://www.activism.net/cypherpunk/manifesto.html>

also available here: https://w2.eff.org/Privacy/Crypto/Crypto_misc/cypherpunk.manifesto

Glencora Borradaile (2021), *Defend Dissent: Digital Suppression and Cryptographic Defense of Social Movements*

<https://open.oregonstate.education/defenddissent/>

related post: <https://blog.torproject.org/book-defend-dissent-with-tor/>



CC0. No rights reserved.

warnings:

- this material is a very brief overview, neither complete nor fully correct.
- mentions of specific software/resources in this material are not recommendations.
- verify the links in this material before using, especially when downloading software.