Network Security and Cryptography
Symmetric-key cryptography

Lecture 11: Ethics of cryptography

Mark Ryan

Ethical questions

Cryptography is a very powerful tool. Therefore, natural questions arise about who should be able to use the tool, for what activities, and whether someone else (for example, law enforcement agencies) should be able to break encryption. This debate has a long and quite complex history.
To make things more concrete, let us focus on an issue much discussed today:

Should short-message services (such as WhatsApp, Telegram, and Signal) be end-to-end encrypted?

"*End-to-end encrypted* means that the sender and the receiver establish a shared symmetric key (e.g., using public-key crypto), and nobody except them can access the key. Therefore, service providers and intermediaries (such as Facebook, Google, ISPs, network operators) are incapable of seeing the plaintext of communications.

End-to-end encryption: two caveats

e2e encryption is powerful, but there are two caveats to bear in mind:

1. It protects message content but not message metadata (who messages whom, with what frequency, in what volume, at what times, etc.).
   - That is Facebook's pact: you get privacy of your content, but we exploit the hell out of your metadata to inform our social network of how people are connected together.
2. It relies on the end-points (Alice and Bob's devices and their software) being secure.
   - There is no way for anyone to verify WhatsApp is really e2e encrypted, because it relies on the correct programming and configuration of the app, the OS, the firmware and the hardware, all of which is proprietary.

Should short-message services (such as WhatsApp, Telegram, and Signal) be end-to-end encrypted?

Context: surveillance society

Surveillant	***Examples ("official")***	***Examples ("unofficial")***
Governments ("Big brother")	• Communications (email, text message, WeChat, telephony, …) • Web activity (what websites you visit, when, what you do on them, etc.) • Location (from your phone, or transport databases) • Financial (payments, etc.)	• Spyware/malware on your devices
Companies ("Middle brother")	• Service provision (FB, Goog, ISPs, phone networks, banks, universities, …) • Website visits, via cookies • FB is a particularly notable example	• Hidden services on your devices
Friends and family ("Little brother")	• Parental control software • Employee tracking software	• MAC address scanning in public locations • Family spying on your phone • Coercion and other abuses

Is this good or bad?

Surveillor	***Good***	***Bad***
Governments ("Big brother")	• Helps combat crime	• Enables abuse by gov't, and by individual officials • Inhibits democracy by stifling debate • Stifles creativity and experimentation • Provides target for hackers
Companies ("Middle brother")	• Provides useful services	• Enables by company and by individual staff members • Provides target for hackers
Friends and family ("Little brother")	• Protects children and other vulnerable people	• Enables coercion and other abuses • Enables crime

Should WhatsApp be end-to-end encrypted?

Academics and civil rights organisations

- Privacy is a absolute human right
- Substantiated targeted breaches may be permitted (but never untargeted breaches)
- There is no way to "weaken" e2ee for governments without also weakening it for attackers.

Civil rights organisations

- Privacy is a human right, but so are safety and security
- For example, e2ee protects children's privacy but also subjects them to abuse[1]

Gov'ts and law enforcement

- Without content interception, police could not have caught David Wilson ("web's most dangerous paedophile")[2].
- NSA chief Keith Alexander: "There's no other way to protect Americans than to collect billions of phone and internet records."

[1] UNICEF Research Brief. `www.unicef-irc.org/publications/1151-what-is-encryption-and-why-does-it-matter-for-children.html`

[2] www.wired.co.uk/article/whatsapp-encryption-child-abuse

Two futures, both undesirable

"Security trumps privacy"

Totalitarian surveillance

All aspects of our lives are monitored. There's CCTV in every bathroom.

"Big brother" controls all communication channels, and perhaps even your brain-computer interface.

BB knows everything you say, do, wish, or think.

No-one is free.

"Privacy trumps security"

Paranoid cypherpunk

Everything is private. All payments are made using anonymous cryptocurrencies.

No-one pays tax; there is no state. No-one can he held accountable. Crimes can effectively be committed without fear of repercussions.

Super-wealthy asset owners control everything, but are unaccountable and act with impunity. No-one can find out who owns what (land, buildings, vehicles, companies, . . .)

Principles for privacy violations

Necessity

- Violation of privacy rights can take place only if it is *necessary*.
- "Necessary" means there is no other way to achieve the goal (e.g., to detect the crime, to provide the service).
- This requires looking at all the ways of achieving the goal, and exploring whether there are ways that do not involve violating the privacy right.

Proportionality

- Violation of privacy rights can take place only if it is *proportionate*.
- "Proportionate" means the harm caused by the privacy violation must not be greater than the benefit of achieving the goal.
- This requires evaluating the harm, and the benefit achieved, and comparing them.

Additional principles for privacy violations

Transparency

When privacy rights are violated,

- the violation is recorded and observable
- the benefits (outcomes) arising from such violations are visible

Transparency must be such that it can't be forged. Correctness of the transparency records must be verifiable by users. Transparency might not be fine-grained (in order to preserve the confidentiality of operations). For example, it might reveal the quantity of decryptions (rather than the individual ones).

Accountability

When privacy rights are violated, the violaters have to explain their reasons and can be sanctioned if they acted incorrectly.

Applicability of transparency/accountability principles

Governments

- Encrypted communication
- Financial transactions
- Transport ticketing (Oyster, Octopus etc.)
- Detecting child sexual abuse material (CSAM)

Corporations

- **Social media identities**
- Corporate email
- Employee geotracking
- **Car insurance**
- **Medical pseudonyms**

Friends and family

- **Family member geotracking**
- Credential management

Distributed decryption

To see how we could implement transparent decryption, we need to understand something called *distributed decryption*.

- In ordinary public key decryption, an agent can establish a public key pk and the corresponding secret key sk.
  - A message encrypted with pk can be decrypted by the holder of sk.

- In public key decryption with distributed decryption, a set of agents can establish their public keys pk_i and sk_i. Then they can combine their public keys into a single public key, pk.
  - A message encrypted with pk can be part-decrypted by the holder of any sk_i. It requires all the holders (or a threshold number of them, according to the set up) to decrypt it fully.

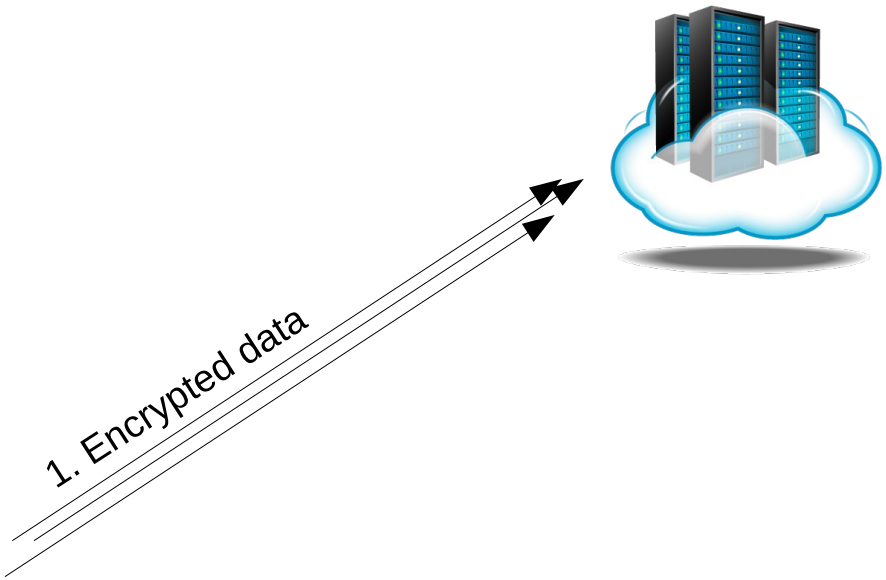
Trustees

Transparent decryption will be done by a set of agents, called trustees.

- Each trustee T_i will establish its public key pk_i and corresponding secret key sk_i.
- Then they will compute their joint public key pk from the individual public keys $pk_1, \ldots, pk_n$.
- This means that anything encrypted with pk can be decrypted only if all (or a threshold number) of trustees each perform their part of the decryption.

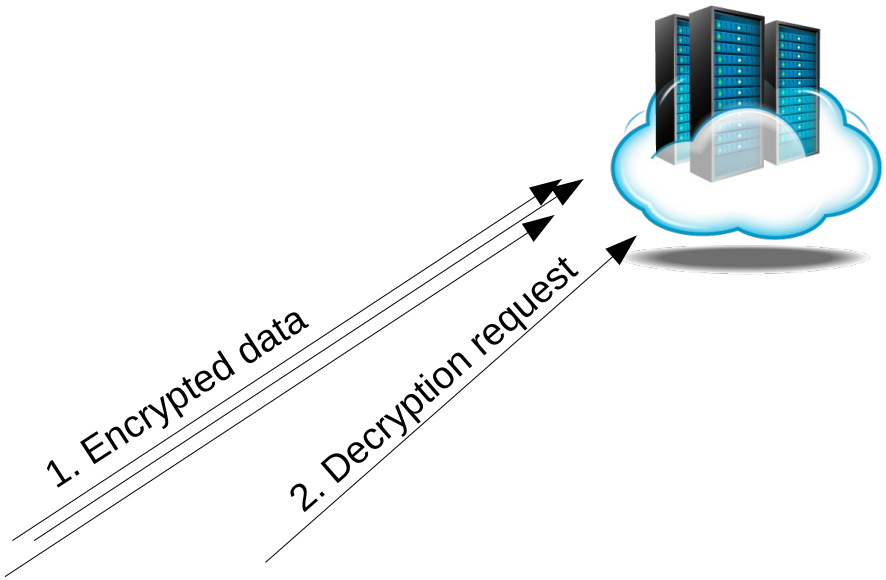
Transparent decryption

- User Alice creates ciphertexts of data s. To do this, the user picks a random session key k and creates the ciphertexts $\mathrm{Enc}_k(s)$ and $\mathrm{Enc}_{pkT}(k)$. Here, pkT is the combined public key of a set of trustees.
- Alice gives $\mathrm{Enc}_k(s)$ and $\mathrm{Enc}_{pkT}(k)$ to decrypting agent Bob.
- At any time, Bob can decrypt, using the following procedure:
  1. He records his decryption request by posting $\mathrm{Enc}_{pkT}(k)$ to the ledger
  2. The trustees see the request on the ledger, and perform their part of the decryption.
  3. After sufficiently many trustees have done that, Bob can combine their results to obtain k.
  4. Bob can now use k to decrypt to get s.
- Alice can detect whether the decryption took place or not, by inspecting the ledger.



Encryptor

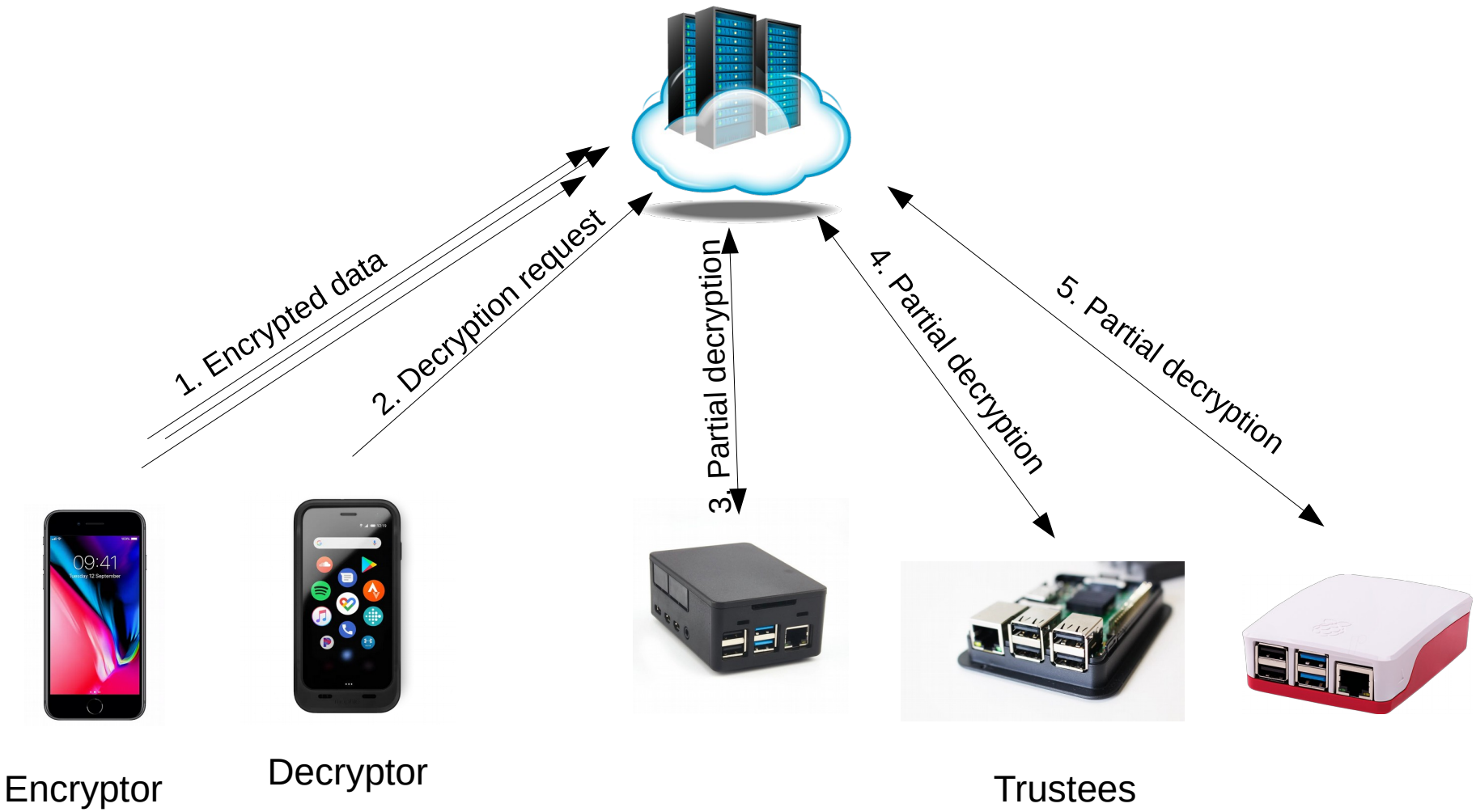
Trustees

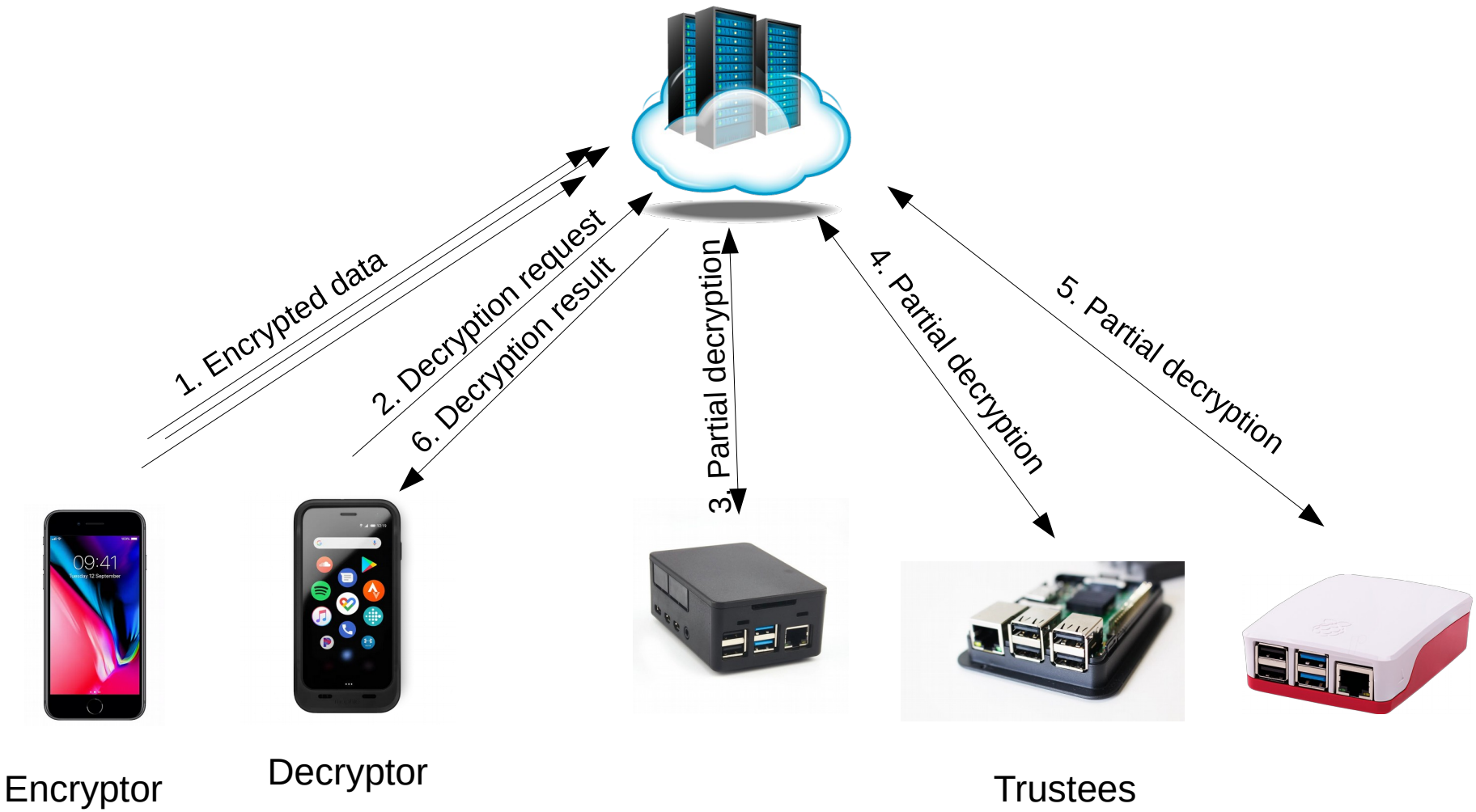


Encryptor

Decryptor

Trustees


1. Encrypted data
2. Decryption request
3. Partial decryption
4. Partial decryption
5. Partial decryption
Encryptor
Decryptor
Trustees


1. Encrypted data
2. Decryption request
6. Decryption result
3. Partial decryption
4. Partial decryption
5. Partial decryption
Encryptor
Decryptor
Trustees

Alice

Bob

Charley

PAD.tech: an opportunity

- A startup company called PAD.tech ("Privacy-preserving accountable decryption") has built an API to support this idea.
- You can get involved by building applications that use it. You can combine this work with your final degree project.
- After your degree, you can possibly be hired by the company.

Interested? Go to pad.tech, or contact me.

Conclusions

1. Privacy is a fundamental right, but even fundamental rights are not absolute rights.

2. Research is needed into how technologies can support making privacy violations transparent and accountable. That means:
   - Making the violations observable
   - Making the outcomes visible intersection).

3. With a London/HK-based company, I am currently developing a community-focussed implementation of the ideas in this talk.

4. I welcome feedback of all kinds!