

Cryptology: Basic concepts and intro

Tanja Lange

Eindhoven University of Technology

2WF80: Introduction to Cryptology

Cryptography

- ▶ Motivation #1: Communication channels are spying on our data.
- ▶ Motivation #2: Communication channels are modifying our data.

Cryptography

- ▶ Motivation #1: Communication channels are spying on our data.
- ▶ Motivation #2: Communication channels are modifying our data.



Cryptography

- ▶ Motivation #1: Communication channels are spying on our data.
- ▶ Motivation #2: Communication channels are modifying our data.



- ▶ Literal meaning of cryptography: “secret writing”.
- ▶ Achieves various security goals by secretly transforming messages.

Cryptographic applications in daily life

- ▶ Credit cards, EC-cards, access codes for Rabobank.
- ▶ Electronic passports or ID cards.
- ▶ Internet commerce, online tax declarations, webmail.
- ▶ Any webpage with `https`.
- ▶ Facebook, WhatsApp, iMessage on iPhone.

Cryptographic applications in daily life

- ▶ Credit cards, EC-cards, access codes for Rabobank.
- ▶ Electronic passports or ID cards.
- ▶ Internet commerce, online tax declarations, webmail.
- ▶ Any webpage with `https`.
- ▶ Facebook, WhatsApp, iMessage on iPhone.
- ▶ PGP encrypted email, Signal, Torbrowser
- ▶ Full disk encryption (iPhone, Bitlocker, ...)
- ▶ Tails, Qubes OS

Cryptographic applications in daily life



- ▶ Credit cards, EC-cards, access codes for Rabobank.
- ▶ Electronic passports or ID cards.
- ▶ Internet commerce, online tax declarations, webmail.
- ▶ Any webpage with https.
- ▶ Facebook, WhatsApp, iMessage on iPhone.
- ▶ PGP encrypted email, Signal, Torbrowser
- ▶ Full disk encryption (iPhone, Bitlocker, ...)
- ▶ Tails, Qubes OS

Snowden in Reddit AmA

Some might say “I don’t care if they violate my privacy; I’ve got nothing to hide.” Help them understand that they are misunderstanding the fundamental nature of human rights. Nobody needs to justify why they “need” a right: the burden of justification falls on the one seeking to infringe upon the right. But even if they did, you can’t give away the rights of others because they’re not useful to you.



Encryption and authentication



- ▶ Simplest case: Alice and Bob share a secret key .
- ▶ Prerequisite: Eve doesn't know .
- ▶ Alice and Bob exchange any number of messages.
- ▶ Encryption takes plaintext m and produces ciphertext c , decryption takes c and produces m so that $\text{Dec}(\text{Enc}(m)) = m$.
- ▶ Security goal #1: **Confidentiality** despite Eve's espionage.



Encryption and authentication



- ▶ Simplest case: Alice and Bob share a secret key .
- ▶ Prerequisite: Eve doesn't know .
- ▶ Alice and Bob exchange any number of messages.
- ▶ Encryption takes plaintext m and produces ciphertext c , decryption takes c and produces m so that $\text{Dec}(\text{Enc}(m)) = m$.
- ▶ Security goal #1: **Confidentiality** despite Eve's espionage.
- ▶ Security goal #2: **Integrity**, i.e., recognizing Eve's sabotage.
- ▶ Security goal #3: **Authenticity**, i.e., recognizing Eve impersonating.

Encryption and authentication



- ▶ Simplest case: Alice and Bob share a secret key .
- ▶ Prerequisite: Eve doesn't know .
- ▶ Alice and Bob exchange any number of messages.
- ▶ Encryption takes plaintext m and produces ciphertext c , decryption takes c and produces m so that $\text{Dec}(\text{Enc}(m)) = m$.
- ▶ Security goal #1: **Confidentiality** despite Eve's espionage.
- ▶ Security goal #2: **Integrity**, i.e., recognizing Eve's sabotage.
- ▶ Security goal #3: **Authenticity**, i.e., recognizing Eve impersonating.
- ▶ Decryption fails for invalid ciphertexts.
(This needs a definition of what "invalid" means).

Goals of cryptography

- ▶ Confidentiality:
Eve cannot learn about the content of the message.
This uses encryption.
- ▶ Integrity:
Eve cannot modify the message without Bob noticing.
If Bob accepts a message it has not been modified
- ▶ Authenticity
Eve cannot impersonate Alice to Bob without Bob noticing.
A message pretending to come from Alice is really from Alice.

Cryptographic tools

Many factors influence the security and privacy of data:

- ▶ Secure storage, physical security; access control.
- ▶ Protection against alteration of data
⇒ **public-key signatures, message-authentication codes.**
- ▶ Protection of sensitive content against reading
⇒ **encryption.**

Cryptology is the science that studies mathematical techniques in order to provide secrecy, authenticity and related properties for digital information.

Many more security goals studied in cryptography

- ▶ Protecting against denial of service.
- ▶ Stopping traffic analysis.
- ▶ Securely tallying votes.
- ▶ Searching in and computing on encrypted data.
- ▶ ...

Cryptanalysis

- ▶ Cryptanalysis is the study of security of cryptosystems.
- ▶ Breaking a system can mean that the hardness assumption was not hard or that it just was not as hard as previously assumed.
- ▶ Breaking can mean recovering the key or the message; or just recovering some information about the key or the message; or fooling Bob into accepting a modified or non-authentic message.
- ▶ Public cryptanalysis is ultimately constructive – ensure that secure systems get used, not insecure ones.
- ▶ Weakened crypto ultimately backfires – we see attacks today because of crypto wars in the 90s.
- ▶ Good arsenal of general approaches to cryptanalysis. There are some automated tools.
- ▶ This area is constantly under development; researchers revisit systems continuously.

x





Cryptology = cryptography + cryptanalysis

- ▶ Cryptography:
Design of cryptosystems (= construction).
This includes implementation of cryptosystems
and their use in larger protocols.

- ▶ Cryptanalysis:
Analysis of cryptosystems (= attacks).
This includes implementation of attacks
and attacks on implementations, e.g., side-channel attacks.