Introduction to cryptography

Daniel Bosk

School of Computer Science and Communication,
KTH Royal Institute of Technology, Stockholm

Department of Information and Communication Systems,
Mid Sweden University, Sundsvall

6th April 2020

- The word has its origin in greek[1]:

  κρυπτός (*kryptos*) meaning hidden[2].

  γράφος (*graphos*) meaning writing[3].

- The area has been around for ages.
- We should not confuse it with *steganography*.
- Steganography concerns hiding a message's *existence*.
- Cryptography concerns hiding a message's *contents*.

---

[1] 'cryptography, n.'. In: *OED Online*. Hämtad den 5 april 2013. Oxford University Press, Mar. 2013. URL: http://www.oed.com/view/Entry/45374?redirectedFrom=cryptography&.

[2] 'crypto-, comb. form'. In: *OED Online*. Hämtad den 5 april 2013. Oxford University Press, Mar. 2013. URL: http://www.oed.com/view/Entry/45363.

[3] 'graphy-, comb. form'. In: *OED Online*. Hämtad den 5 april 2013. Oxford University Press, Mar. 2013. URL: http://www.oed.com/view/Entry/80855.

- The word has its origin in greek[1]:

  κρυπτός (*kryptos*) meaning hidden[2].

  γράφος (*graphos*) meaning writing[3].

- The area has been around for ages.
- We should not confuse it with *steganography*.
- Steganography concerns hiding a message's *existence*.
- Cryptography concerns hiding a message's *contents*.

---

[1] 'cryptography, n.'. In: *OED Online*. Hämtad den 5 april 2013. Oxford University Press, Mar. 2013. URL: http://www.oed.com/view/Entry/45374?redirectedFrom=cryptography&.

[2] 'crypto-, comb. form'. In: *OED Online*. Hämtad den 5 april 2013. Oxford University Press, Mar. 2013. URL: http://www.oed.com/view/Entry/45363.

[3] 'graphy-, comb. form'. In: *OED Online*. Hämtad den 5 april 2013. Oxford University Press, Mar. 2013. URL: http://www.oed.com/view/Entry/80855.

- The word has its origin in greek[1]:

  κρυπτός (*kryptos*) meaning hidden[2].

  γράφος (*graphos*) meaning writing[3].
- The area has been around for ages.
- We should not confuse it with *steganography*.
- Steganography concerns hiding a message's *existence*.
- Cryptography concerns hiding a message's *contents*.

---

[1] 'cryptography, n.'. In: *OED Online*. Hämtad den 5 april 2013. Oxford University Press, Mar. 2013. URL: http://www.oed.com/view/Entry/45374?redirectedFrom=cryptography&.

[2] 'crypto-, comb. form'. In: *OED Online*. Hämtad den 5 april 2013. Oxford University Press, Mar. 2013. URL: http://www.oed.com/view/Entry/45363.

[3] 'graphy-, comb. form'. In: *OED Online*. Hämtad den 5 april 2013. Oxford University Press, Mar. 2013. URL: http://www.oed.com/view/Entry/80855.

- Then it was an art, now it's a science.
- People used 'clever' constructions.
- These were thought to be secure: 'How can anyone figure this out?'
- Well, it turns out that there are always a lot of people with a lot of time and motivation . . .

- Then it was an art, now it's a science.
- People used 'clever' constructions.
- These were thought to be secure: 'How can anyone figure this out?'
- Well, it turns out that there are always a lot of people with a lot of time and motivation . . .

- Then it was an art, now it's a science.
- People used 'clever' constructions.
- These were thought to be secure: 'How can anyone figure this out?'
- Well, it turns out that there are always a lot of people with a lot of time and motivation ...

A quote[4]

[A cryptosystem] should not require secrecy, and it should not be a problem if it falls into the enemy hands;

Kerckhoff's Principle

- No security-by-obscurity
- The key should be the only secret

[4] Auguste Kerckhoff. 'La cryptographie militaire'. In: *Journal des sciences militaires* 9 (1883), pp. 5–38, 161–191.

A quote[4]

[A cryptosystem] should not require secrecy, and it should not be a problem if it falls into the enemy hands;

Kerckhoff's Principle

- No security-by-obscurity
- The key should be the only secret

[4] Auguste Kerckhoff. 'La cryptographie militaire'. In: *Journal des sciences militaires* 9 (1883), pp. 5–38, 161–191.

Note

- This doesn't mean we must tell the adversary what we're using.
- But we shouldn't loose any security if we do.

Shared-key Stems from the classical crypto where a key is shared between two users.

Public-key This is more modern crypto, from 1970s. Each user has a public and a private key.

Counter-intuitive More modern, from 1980s and onwards. How to do computations on secret inputs, prove knowledge without revealing of what.

Shared-key Stems from the classical crypto where a key is shared between two users.

Public-key This is more modern crypto, from 1970s. Each user has a public and a private key.

Counter-intuitive More modern, from 1980s and onwards. How to do computations on secret inputs, prove knowledge without revealing of what.

Shared-key Stems from the classical crypto where a key is shared between two users.

Public-key This is more modern crypto, from 1970s. Each user has a public and a private key.

Counter-intuitive More modern, from 1980s and onwards. How to do computations on secret inputs, prove knowledge without revealing of what.

[1] ‘cryptography, n.’. In: *OED Online*. Hämtad den 5 april 2013. Oxford University Press, Mar. 2013. URL: http://www.oed.com/view/Entry/45374?redirectedFrom=cryptography&.

[2] ‘crypto-, comb. form’. In: *OED Online*. Hämtad den 5 april 2013. Oxford University Press, Mar. 2013. URL: http://www.oed.com/view/Entry/45363.

[3] ‘graphy-, comb. form’. In: *OED Online*. Hämtad den 5 april 2013. Oxford University Press, Mar. 2013. URL: http://www.oed.com/view/Entry/80855.

[4] Auguste Kerckhoff. ‘La cryptographie militaire’. In: *Journal des sciences militaires* 9 (1883), pp. 5–38, 161–191.