E-MAIL ENCRYPTION

ROB‘S TECHNICAL SEMINAR

02.05.2014

Dominik Klaes

Outline

- What is encryption? / Why do we need it?
- How does encryption work?
- Let‘s do it!

What is encryption? / Why do we need it?

What and why?

- Encryption means making information unreadable for unathorized people and only accessible for you and authorized people
- Why? Some things should be kept secret. There are enough (very) good reasons.
- Signing messages! You might want to know if the other one if he/she is the one you expect.

How does encryption work?

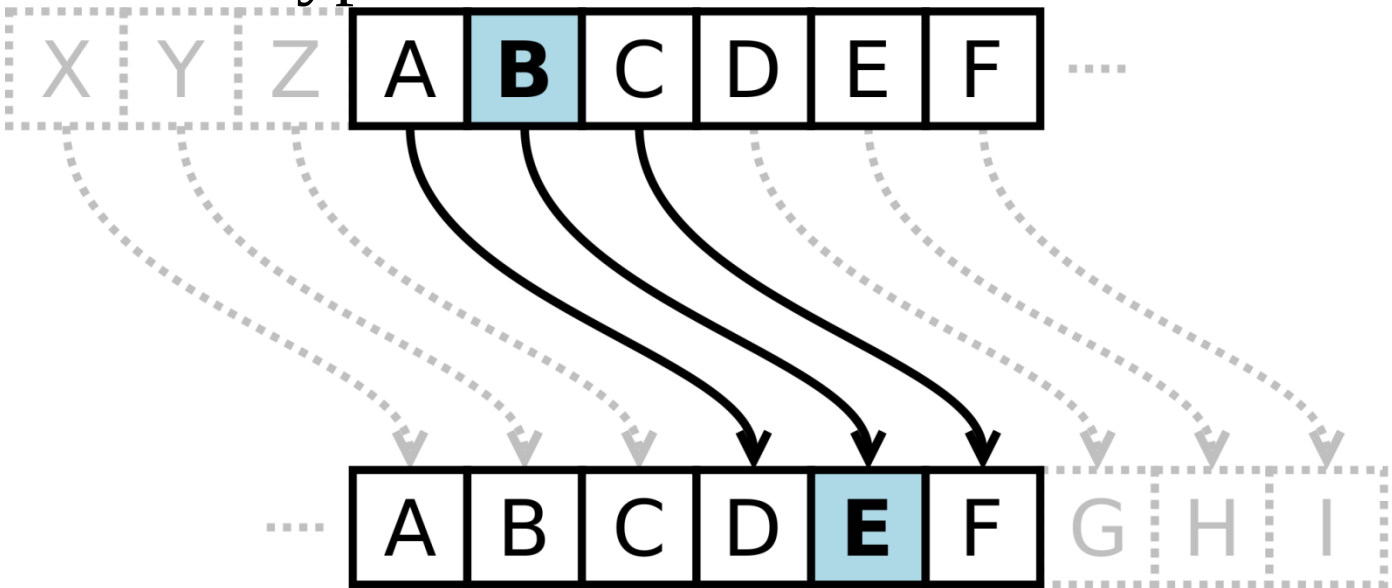
How does encryption work?

- Encrypt and decrypt with same key (symmetric encryption)
- Encrypt and decrypt with two different keys (asymmetric encryption)

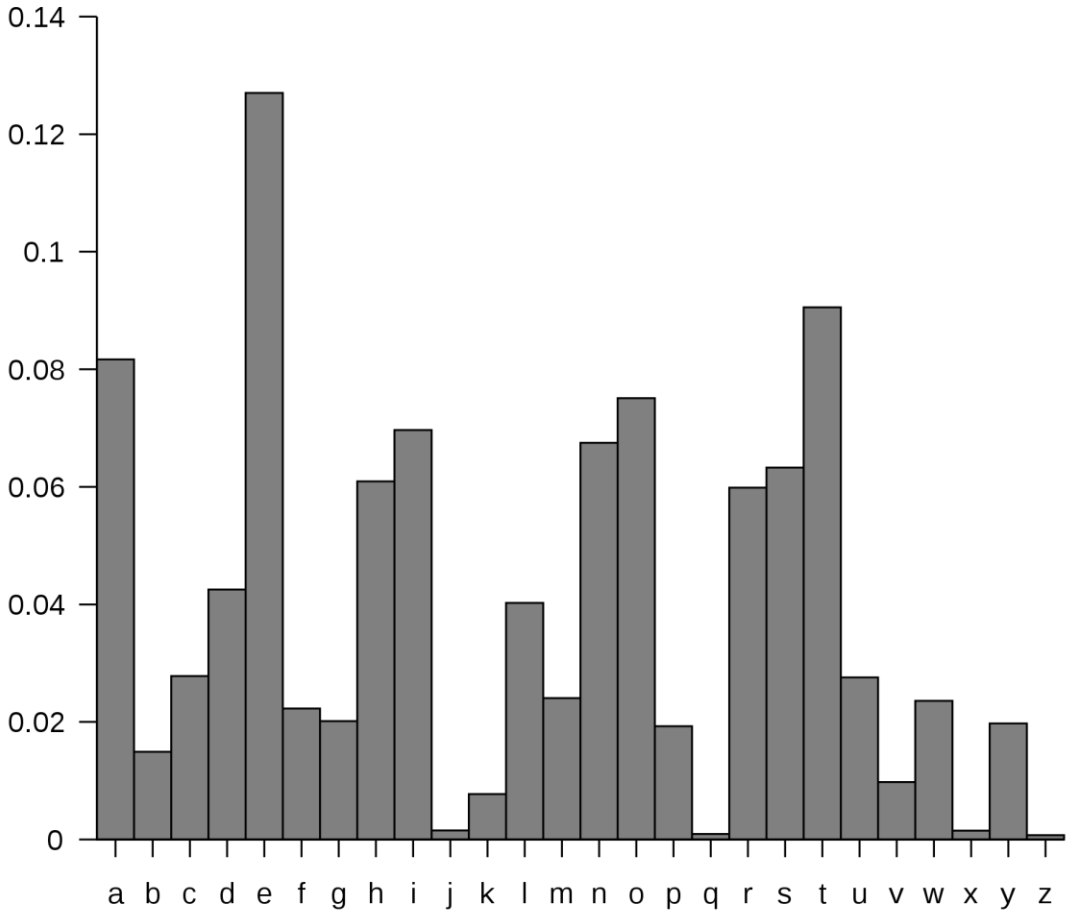
- Tools available for all important mail clients and also for GoogleChrome (for encryption of e.g. Facebook messages!) and smartphones!

Examples (1)

- Words backwards:
  - hello -> olleh
- Other language
  - Can you read hieroglyphics?
- Caesar encryption:



Examples (2)



Number of letters in an English text

Examples (3)

- State of the art: RSA, asymmetric
  - Combination of public and private key
  - Encrypt message with public key of recipient.
  - Only the recipient can decrypt the message with his/her private key!
  - Sign your message with your private key.
  - Signature can be verified by using public key.
  - You have to trust the public key (you have to know once that the other one is the right person).

Examples (4): RSA (1)

- Choose two prime numbers p and q.
  - p = 11 and q = 13
- Calculate the RSA modul N
  - N = p * q = 11 * 13 = 143
- Calculate Euler's φ function
  - φ(N) = φ(143) = (p – 1)(q – 1) = 120
- Choose an e that is coprime to φ(N)
  - e = 23
- **N and e are the public key!**

Examples (5): RSA (2)

- Calculate the inverse to e:
  - $e * d + k * \varphi(N) = 1 = \gcd(e, \varphi(N))$
  - $23 * d + k * 120 = 1 = \gcd(e, \varphi(N))$
  - Using “Extended Euclidean algorithm”:
    - $d = 47$
    - $k = -9$
  - **d is your private key (k is not longer needed)!**

Examples (6): RSA (3)

Let's encrypt (public key) and decrypt (private key)!

- c is the encrypted message, m the message.
  - Let's say m = 7.
  - $c = m^e \pmod N$ $\qquad\qquad$ $m < N$!
  - $2 = 7^{23} \pmod{143}$
- Now decrypt:
  - $m = c^d \pmod N$
  - $7 = 2^{47} \pmod{143}$

Let‘s do it!

Questions?