An Introduction to Cryptology

Prof. Bart Preneel

Katholieke Universiteit Leuven, Belgium

Bart.Preneel@esat.kuleuven.ac.be

http://www.esat.kuleuven.ac.be/~preneel

Slides used by permission

Comp527 status items

- Voting machine project is out
  - Does everybody have a partner?
- Next three weeks: crash course in cryptography and crypto-protocols

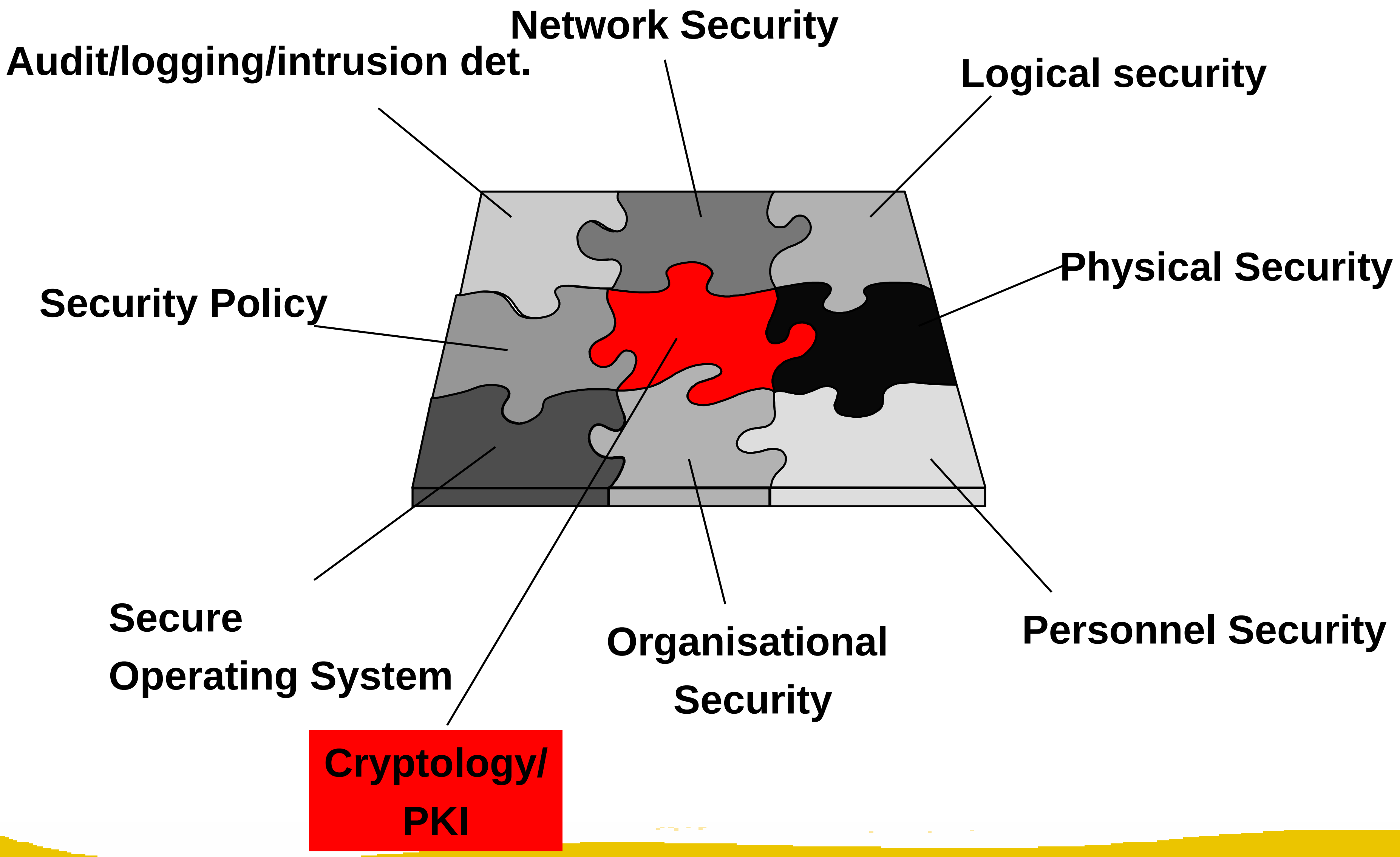
Some books on cryptology

- B. Schneier, Applied Cryptography, Wiley, 1996. Widely popular and very accessible – make sure you get the errata.
- D. Stinson, Cryptography: Theory and Practice, CRC Press, 1995. Solid introduction, but only for the mathematically inclined.
  - 2nd edition, part 1 available in 2002.
- A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1997. The bible of modern cryptography. Thorough and complete reference work – not suited as a first text book. All chapters can be downloaded for free at http://www.cacr.math.uwaterloo.ca/hac

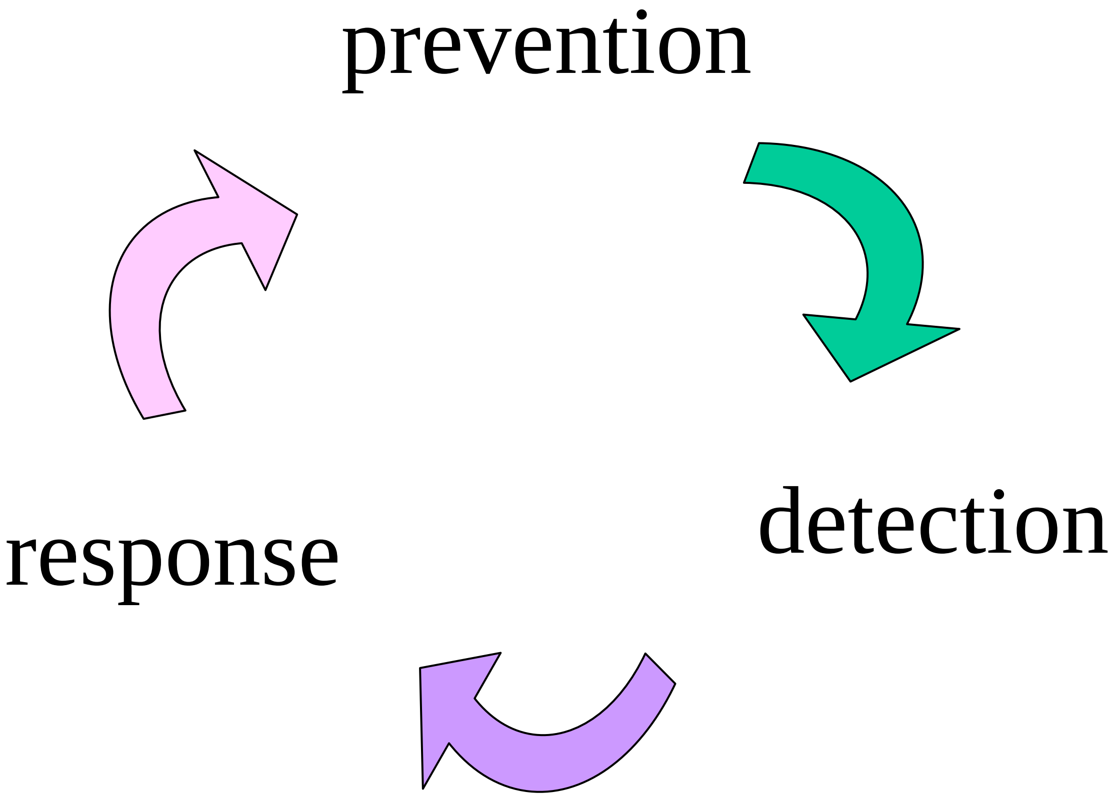
More information: some links

- IACR (International Association for Cryptologic Research): www.iacr.org
- IETF web site: www.ietf.org
- Cryptography faq: www.faqs.org/faqs/cryptography-faq
- links: Ron Rivest, David Wagner, Counterpane www.counterpane.com/hotlist.html
- Digicrime (www.digicrime.org) - not serious but informative and entertaining

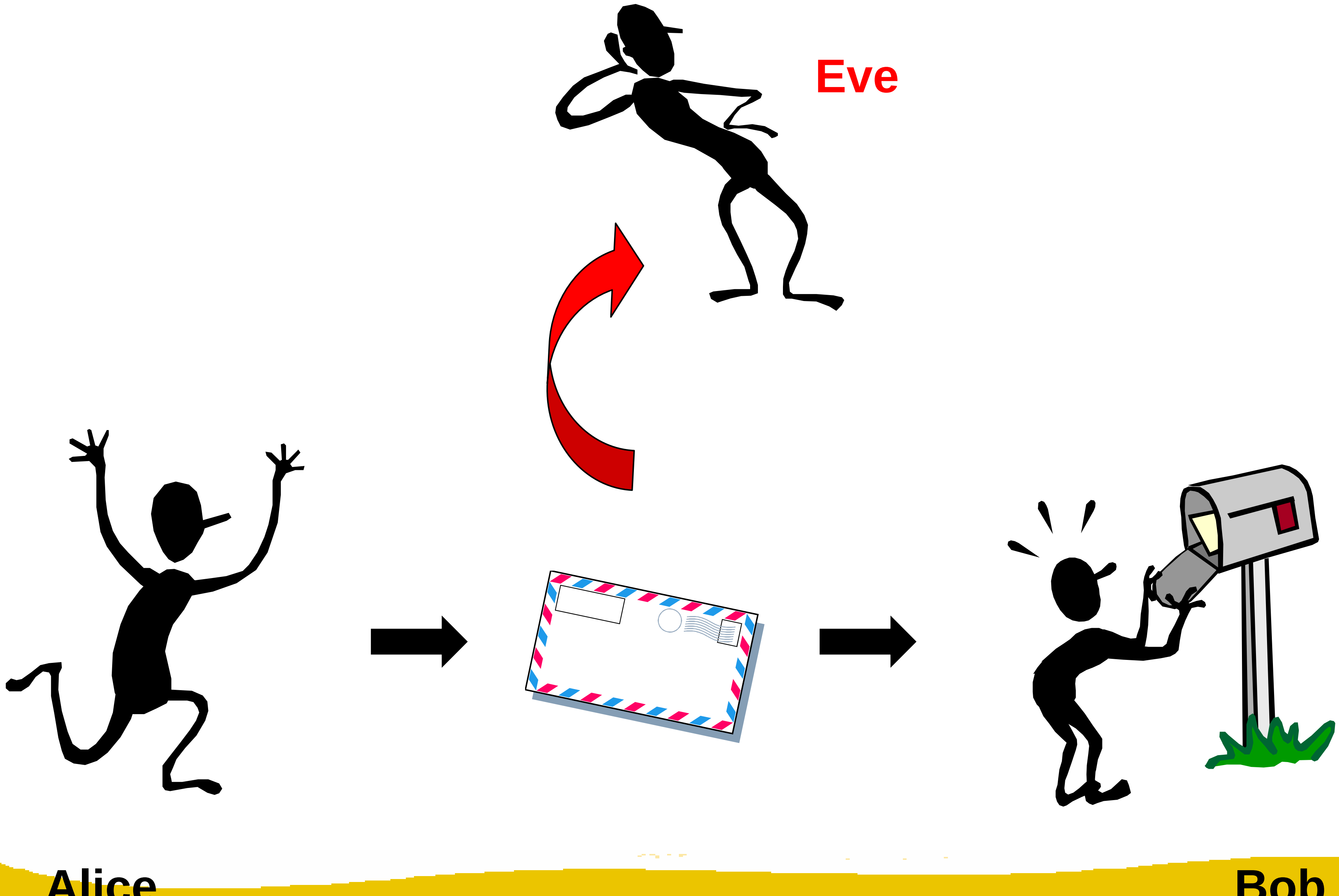
Information security: a puzzle



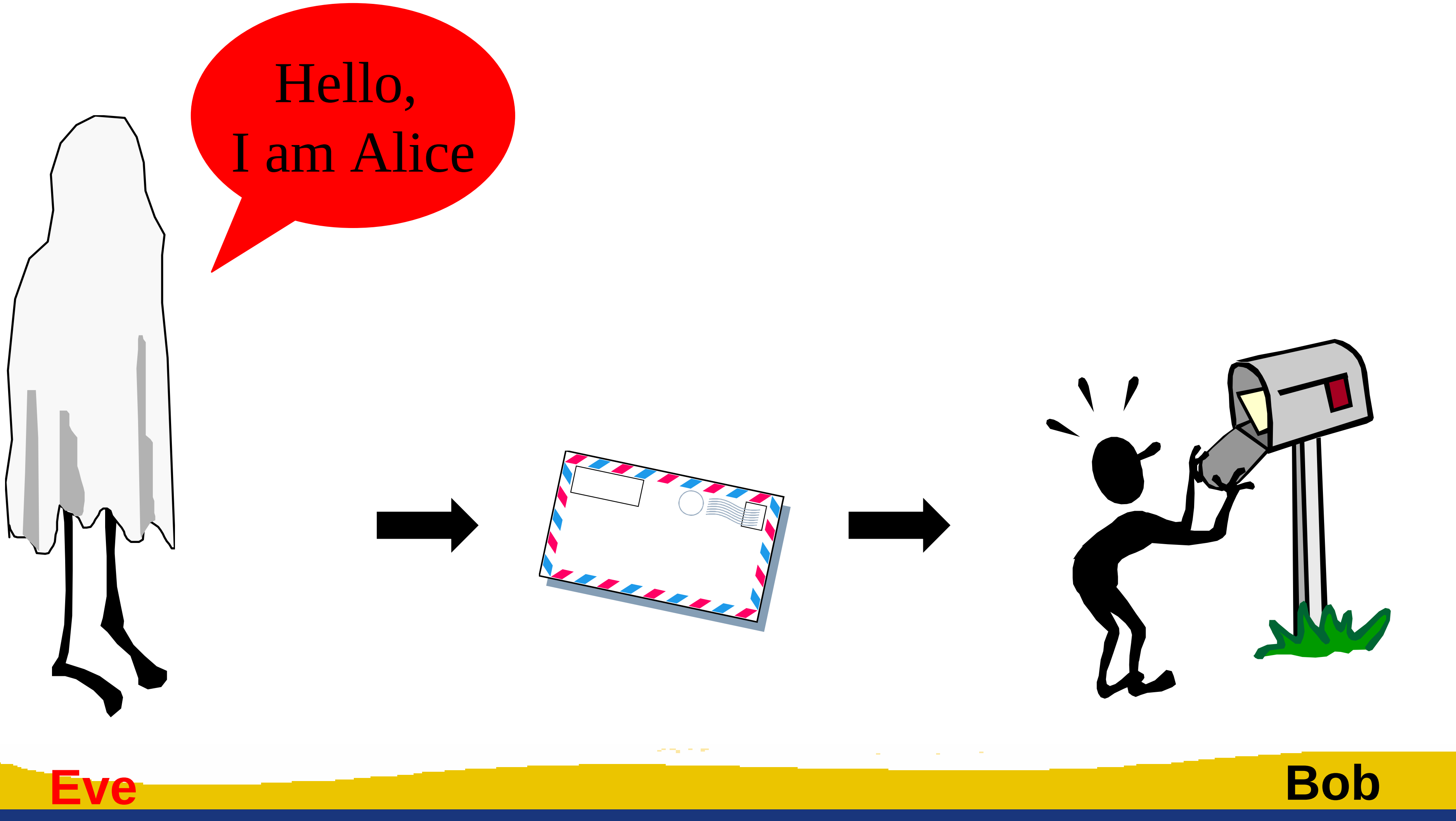
Process approach to security



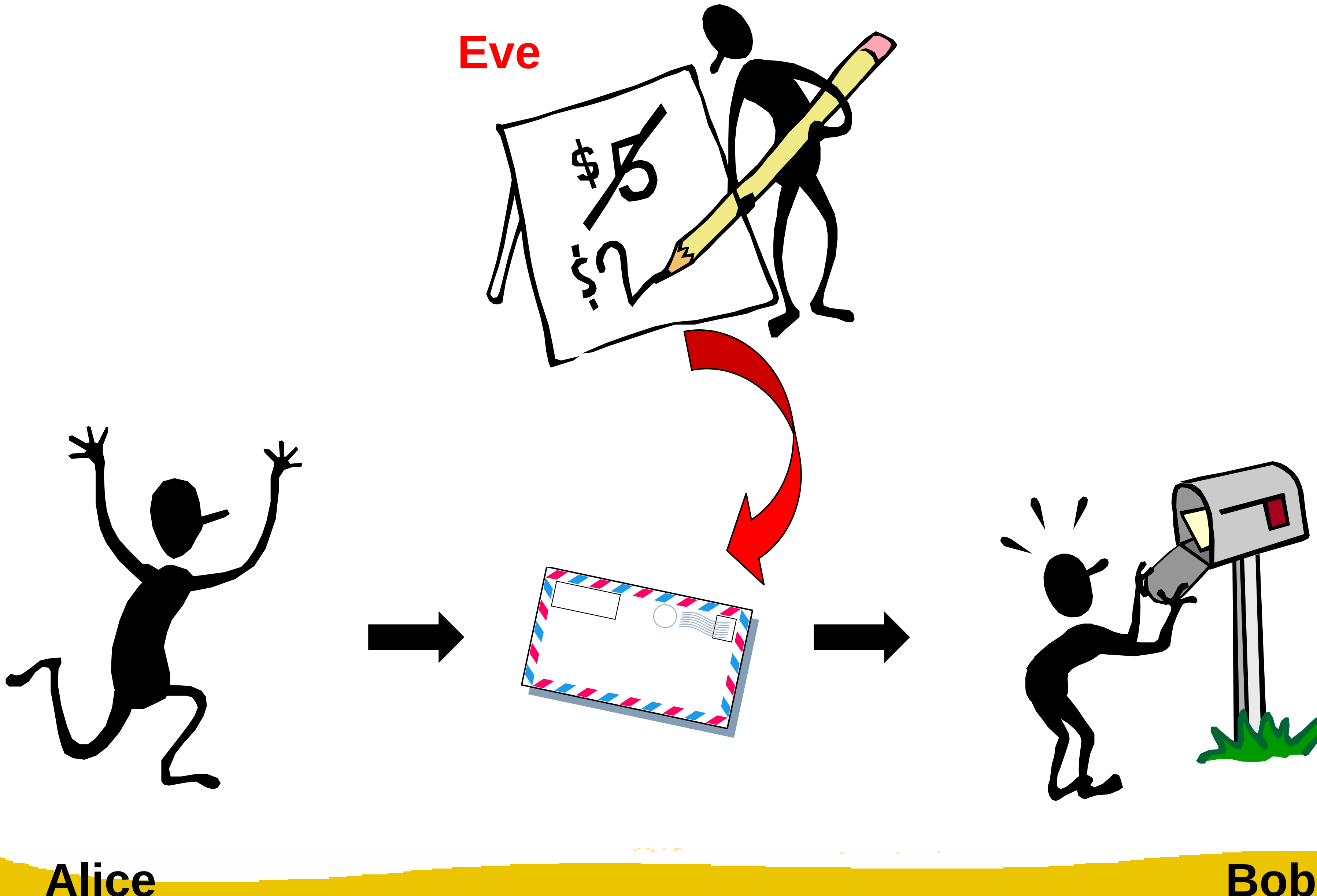
Data confidentiality



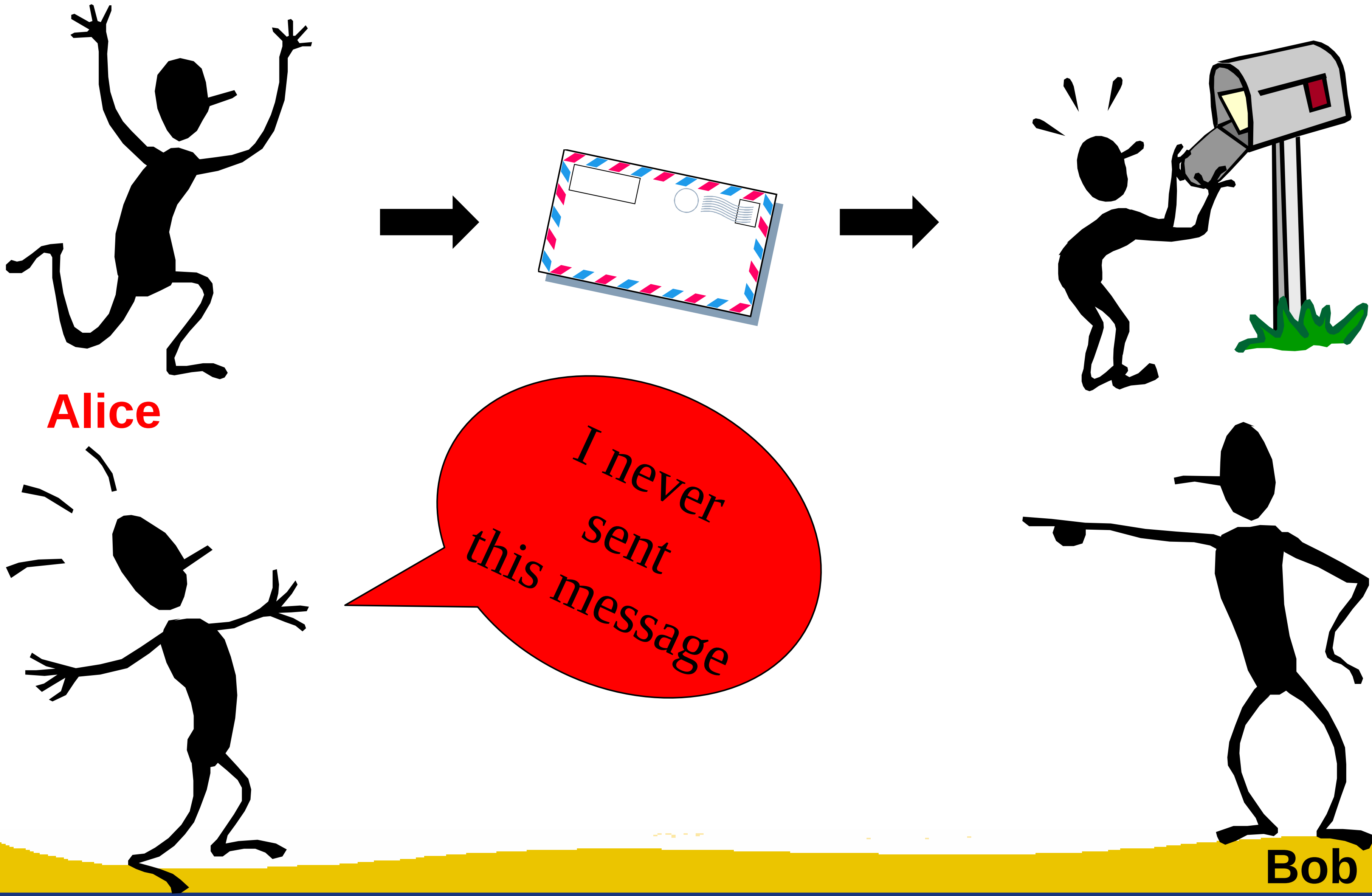
Entity authentication



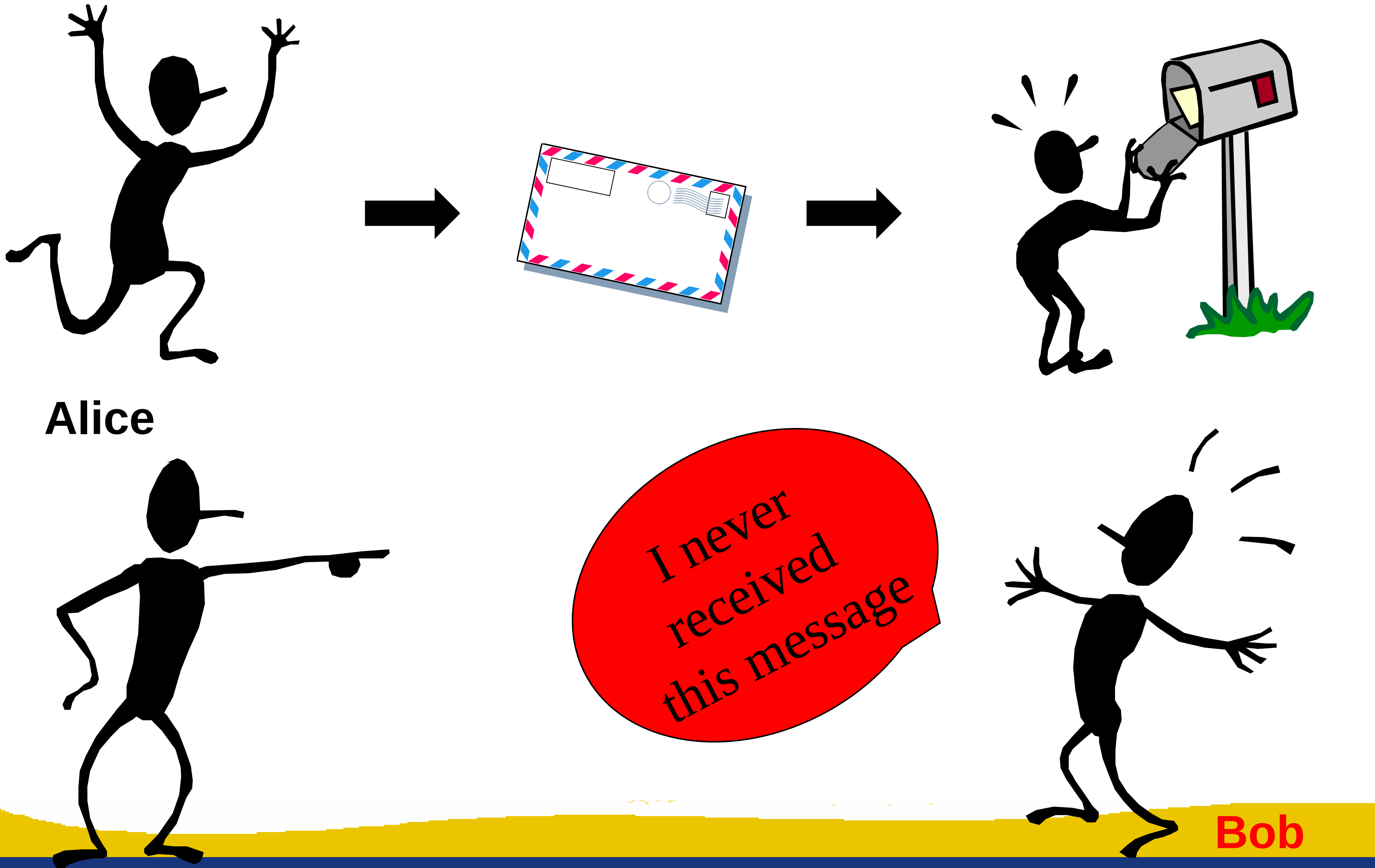
Data authentication



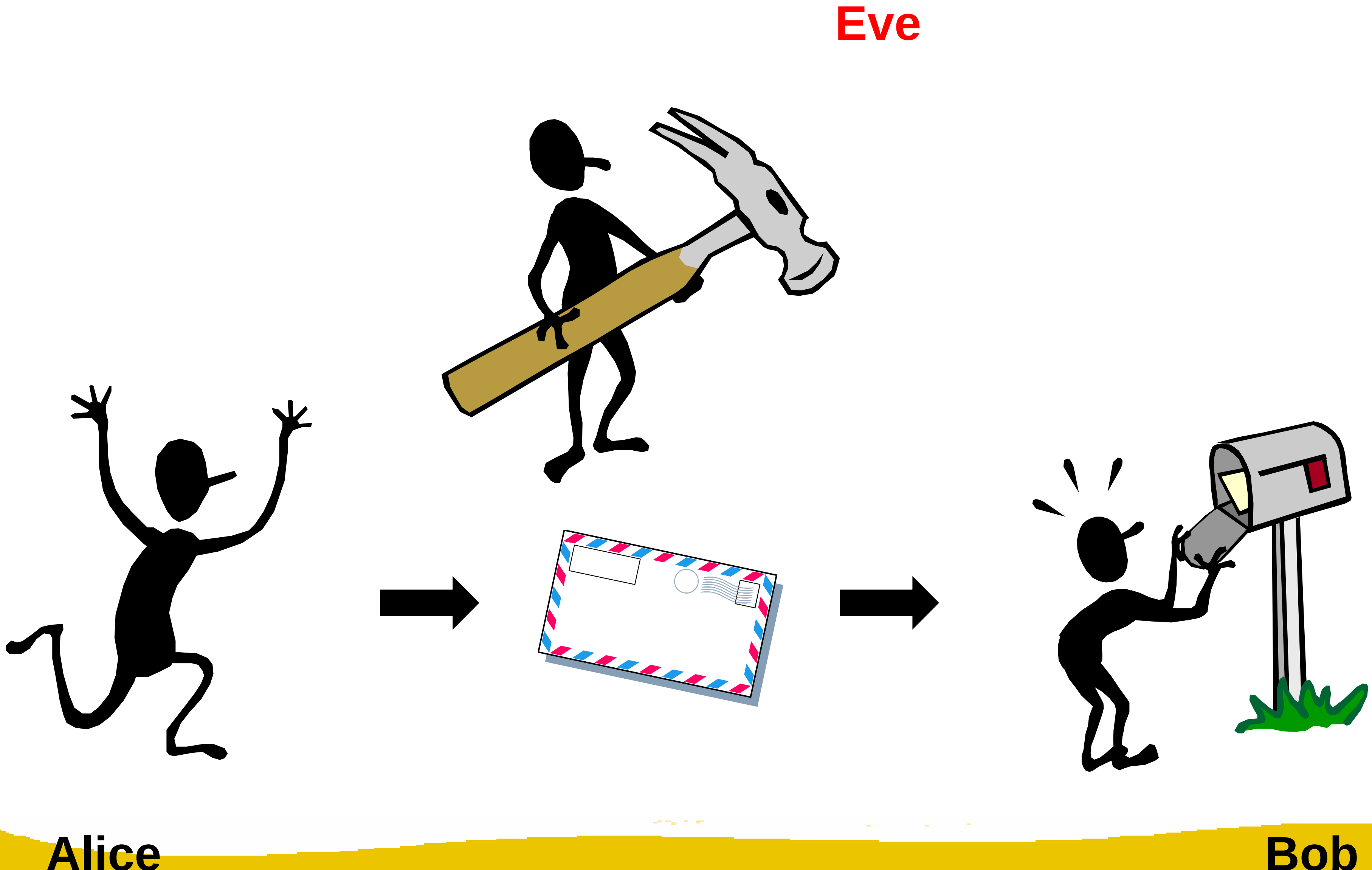
Non-repudiation (origin)



Non-repudiation (receipt)



Denial of service



Definitions

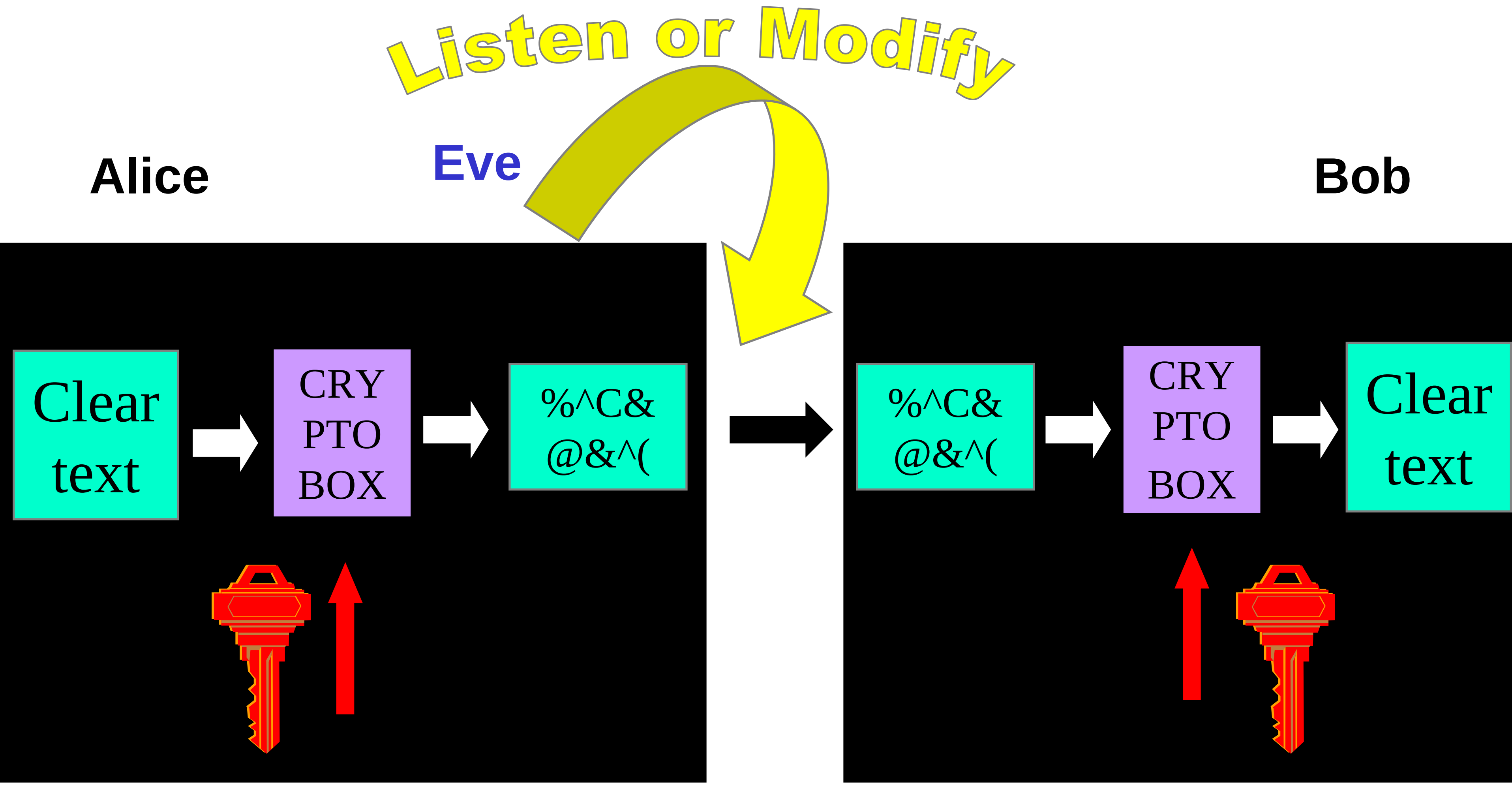
	data	**entities**
confidentiality	encryption	anonymity
authentication	data authentication	identification

Non-repudiation of origin, receipt

Contract signing

Notarisation and Timestamping

Cryptology: basic principles



Symmetric cryptology: confidentiality

- old cipher systems:
  - transposition, substitution, rotor machines
- the opponent and her power
- the Vernam scheme
- A5/1, Bluetooth, RC4
- DES and triple-DES
- AES

Old cipher systems (pre-1900)

- Caesar cipher: shift letters over k positions in the alphabet (k is the secret key)

```
THIS IS THE CAESAR CIPHER
WKLV LV WKH FDHVDU FLSKHU
```

- Julius Caesar never changed his key (k=3).

Cryptanalysis example:

```
HJAEG JAWFW FNGQW JMKMJ
IKBFH KBXGX GOHRX KNLNK
JLCGI LCYHY HPISY LOMOL
KMDHJ MDZIZ IQJTZ MPNPM
LNEIK NEAJA JRKUA NQOQN
MOFGL OFBKB KSLVB ORPRO
NPGHM PGCLC LTMWC PSQSP
OQHLN QHDMD MUNXD QTRTQ
PRIMO RIENE NVOYE RUSUR
QSJNP SJFOF OWPZF SVTVS
RTKOQ TKGPG PXQAG TWUWT
```

Old cipher systems (pre-1900) (2)

- Substitutions
  - ABCDEFGHIJKLMNOPQRSTUVWXYZ
  - MZNJSOAXFQGYKHLUCTDVWBIPER
- Transpositions

TRANS	ORI S
POSIT	NOTIT
IONS	OSANP

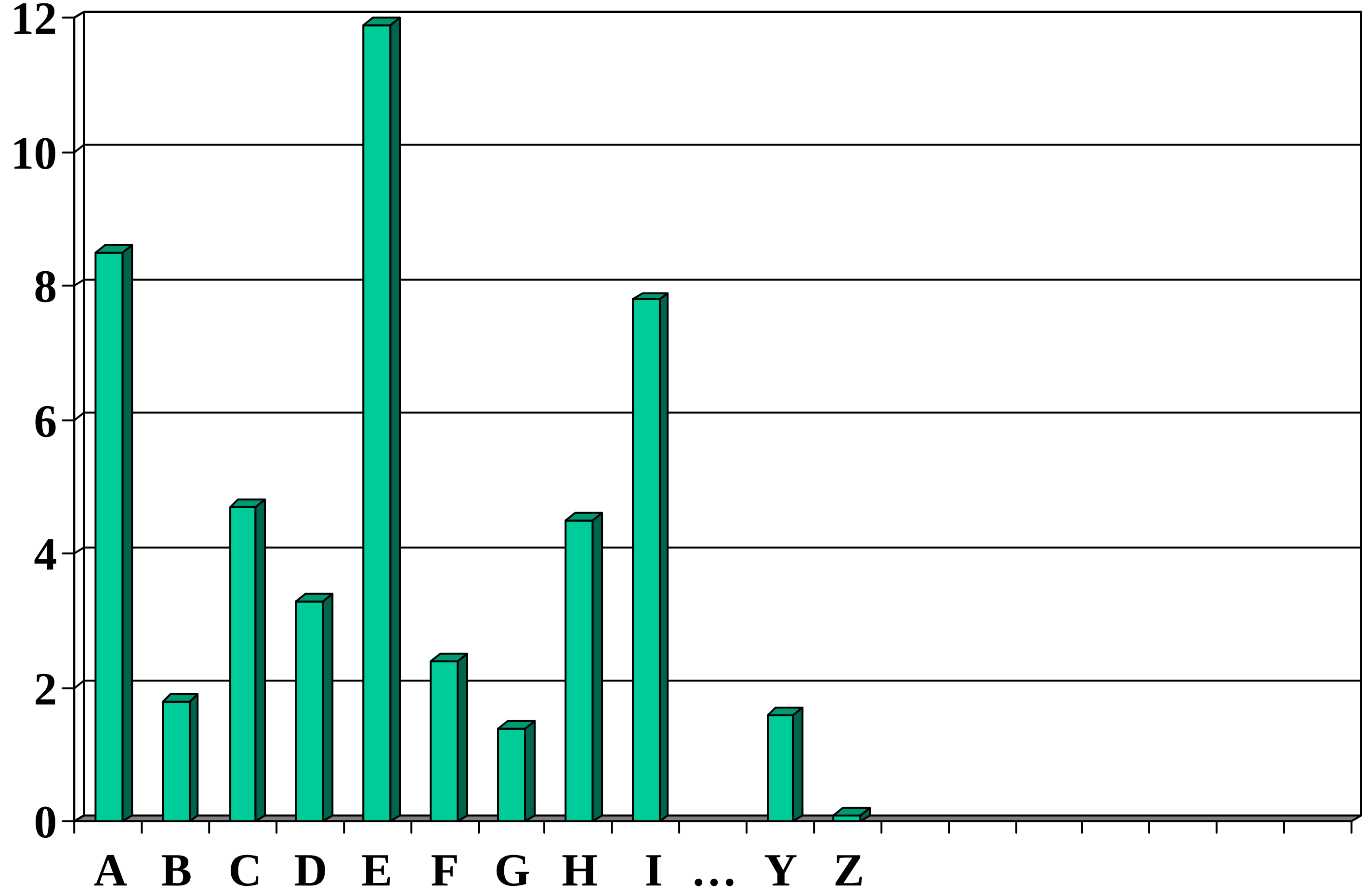
Security

- there are n! different substitutions on an alphabet with n letters
- there are n! different transpositions of n letters
- n=26:

  n!=403291461126605635584000000 = 4 10^{26} keys
- trying all possibilities at 1 nanosecond per key requires....

Easy to break simple subsitution using statistical techniques

Letter distributions



Assumptions on Eve (the opponent)

- Cryptology = cryptography + cryptanalysis
- Eve knows the algorithm, except for the key (Kerckhoffs's principle)
- increasing capability of Eve:
  - knows some information about the plaintxt (e.g., in English)
  - knows part of the plaintext
  - can choose (part of) the plaintext and look at the ciphertext
  - can choose (part of) the ciphertext and look at the plaintext

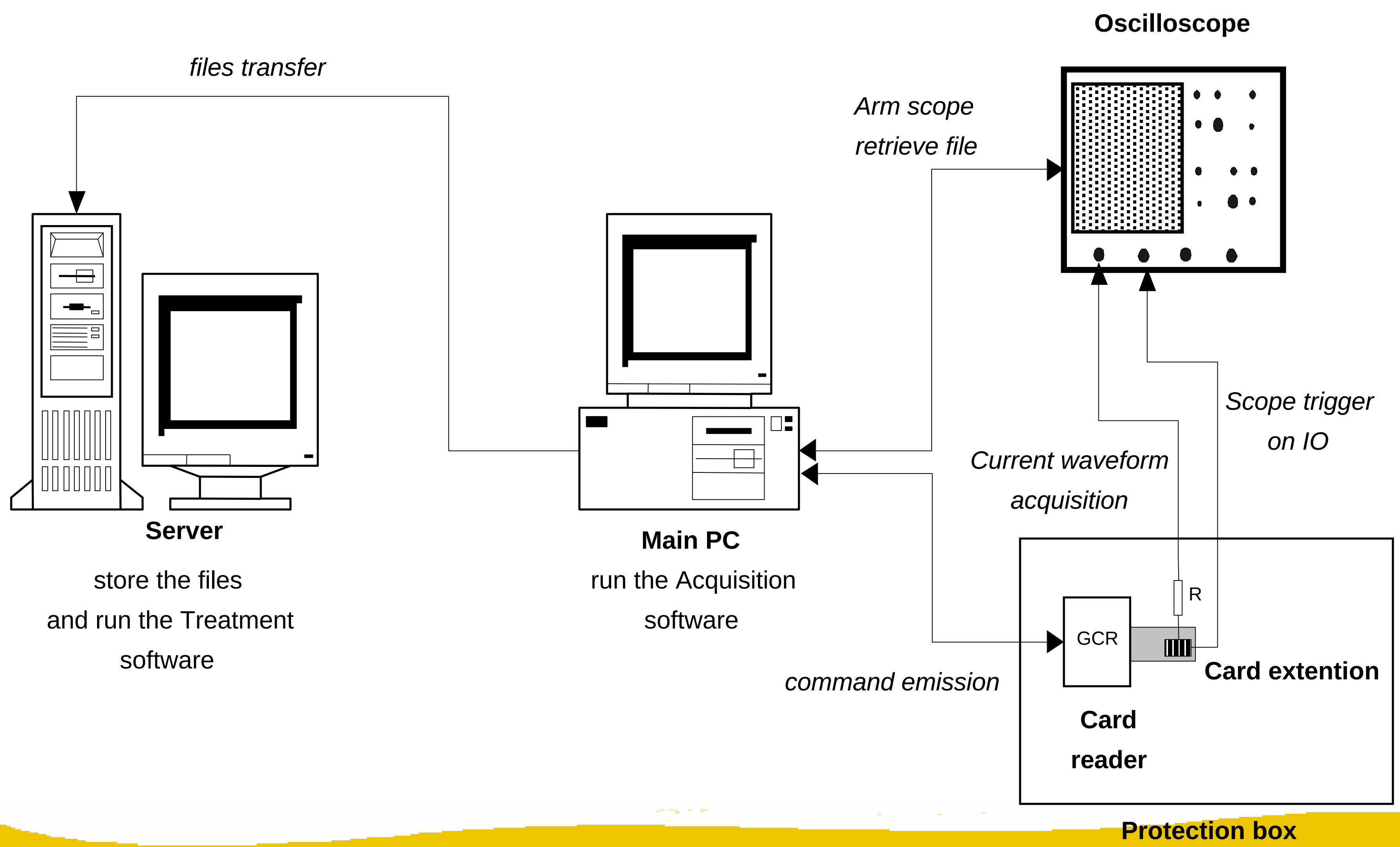
Assumptions on Eve (the opponent)

- A scheme is broken if Eve can deduce the key or obtain additional plaintext
- Eve can always try all possible keys till "meaningful" plaintext appears:
  a brute force attack
  - solution: large key space
- Eve will try to find shortcut attacks (faster than brute force)
  - history shows that designers are too optimistic about the security of their cryptosystems

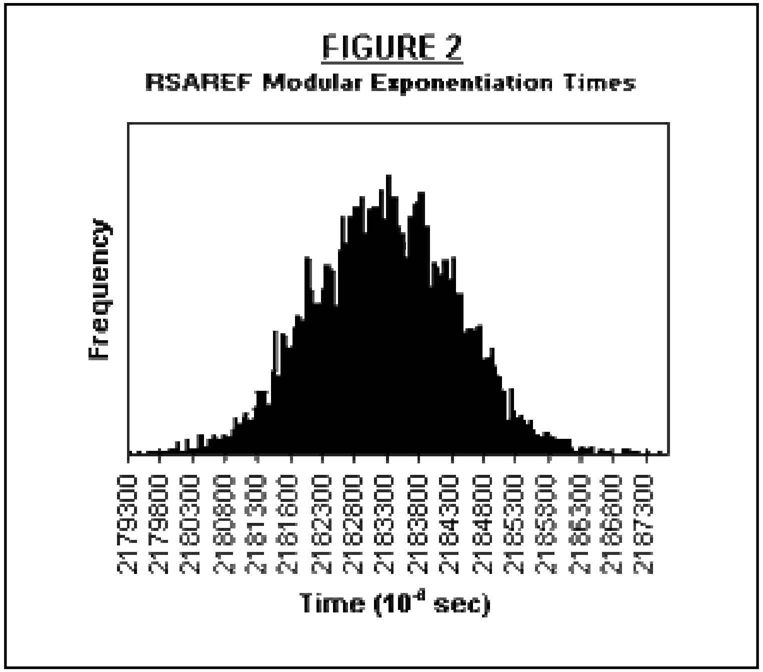
New assumptions on Eve

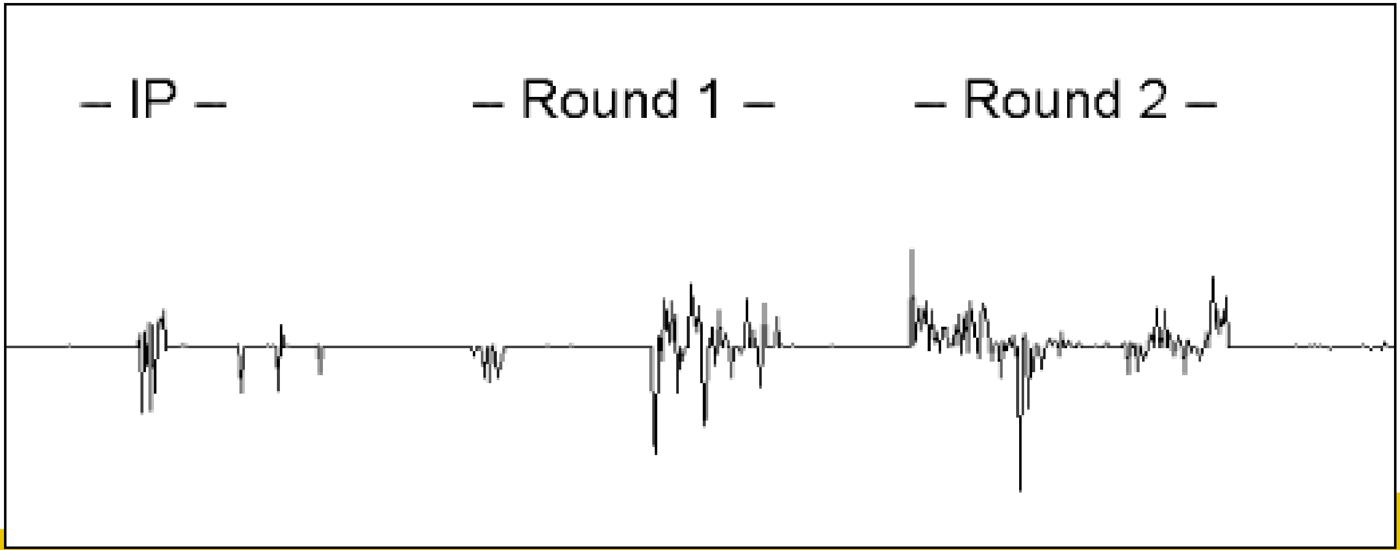
- Eve may have access to side channels
  - timing attacks
  - simple power analysis
  - differential power analysis
  - differential fault analysis
  - electromagnetic interference

Side channel analysis

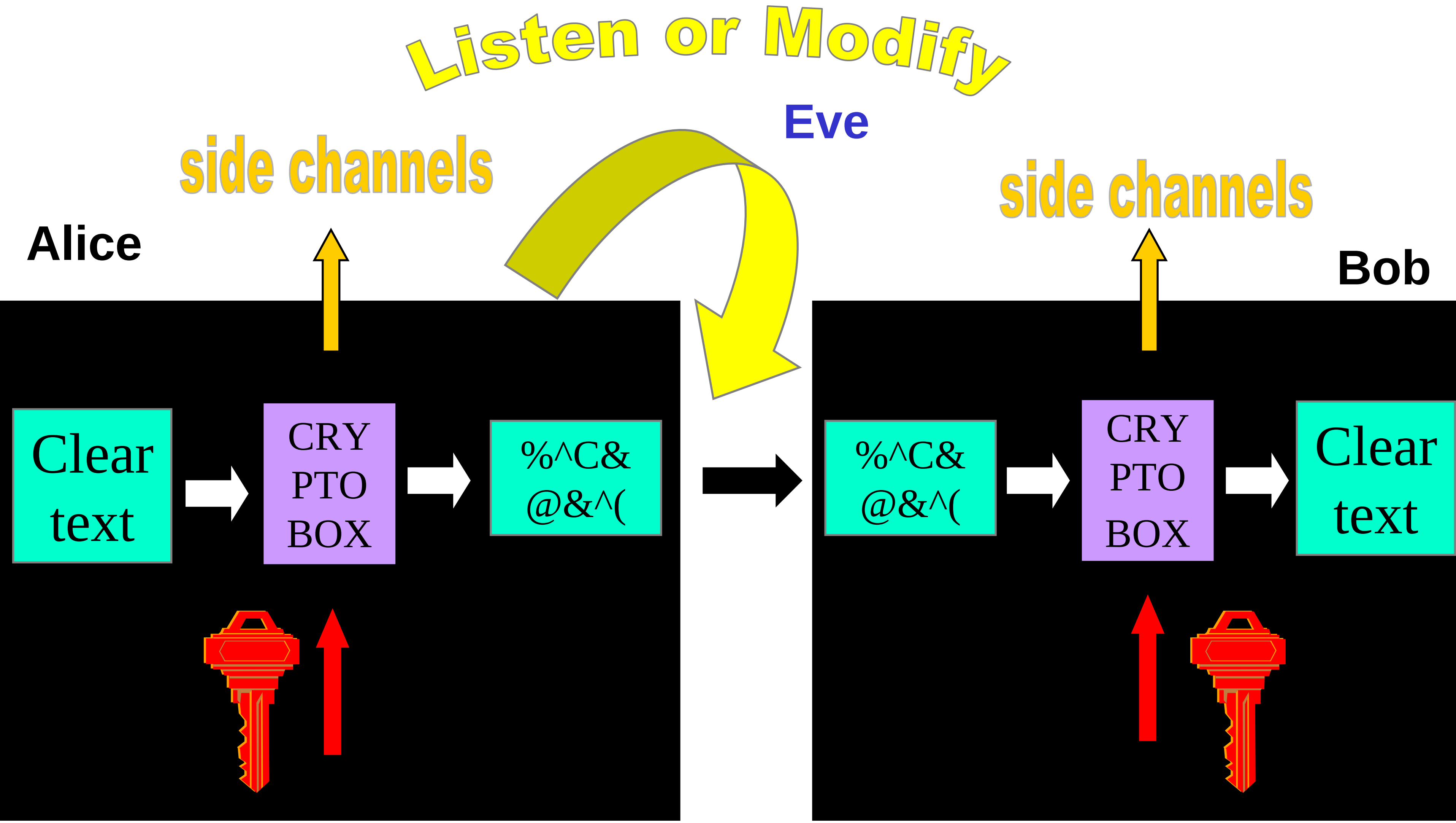


Timing attacks and power analysis



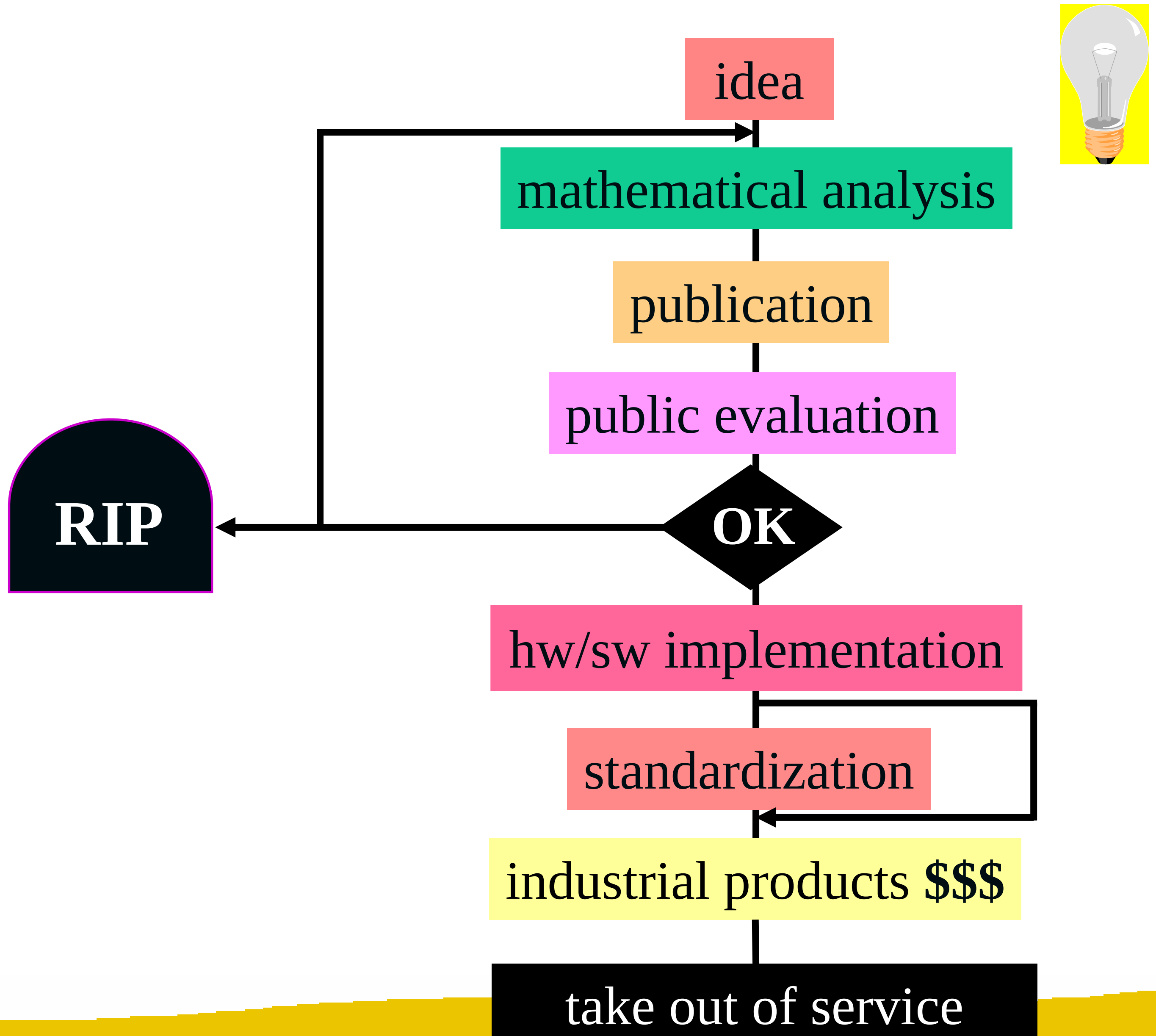


Cryptology + side channels



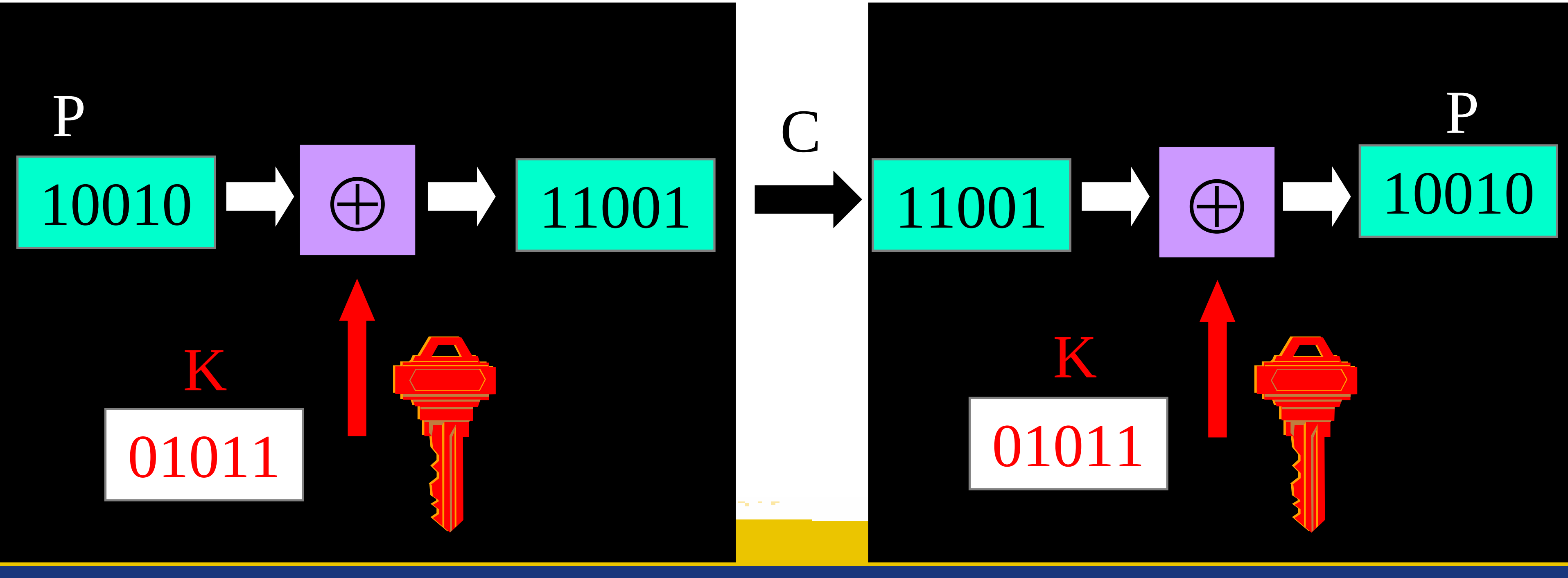
The Rotor machines (WW II)

Life cycle of a cryptographic algorithm



Vernam scheme (1917) + Shannon (1948)

- key is random string, as long as the plaintext



Vernam scheme

- perfect secrecy: ciphertext gives opponent no additional information on the plaintext or $H(P|C)=H(P)$
- impractical: key is as long as the plaintext
- but this is optimal: for perfect secrecy $H(K) \geq H(P)$

Three approaches in cryptography

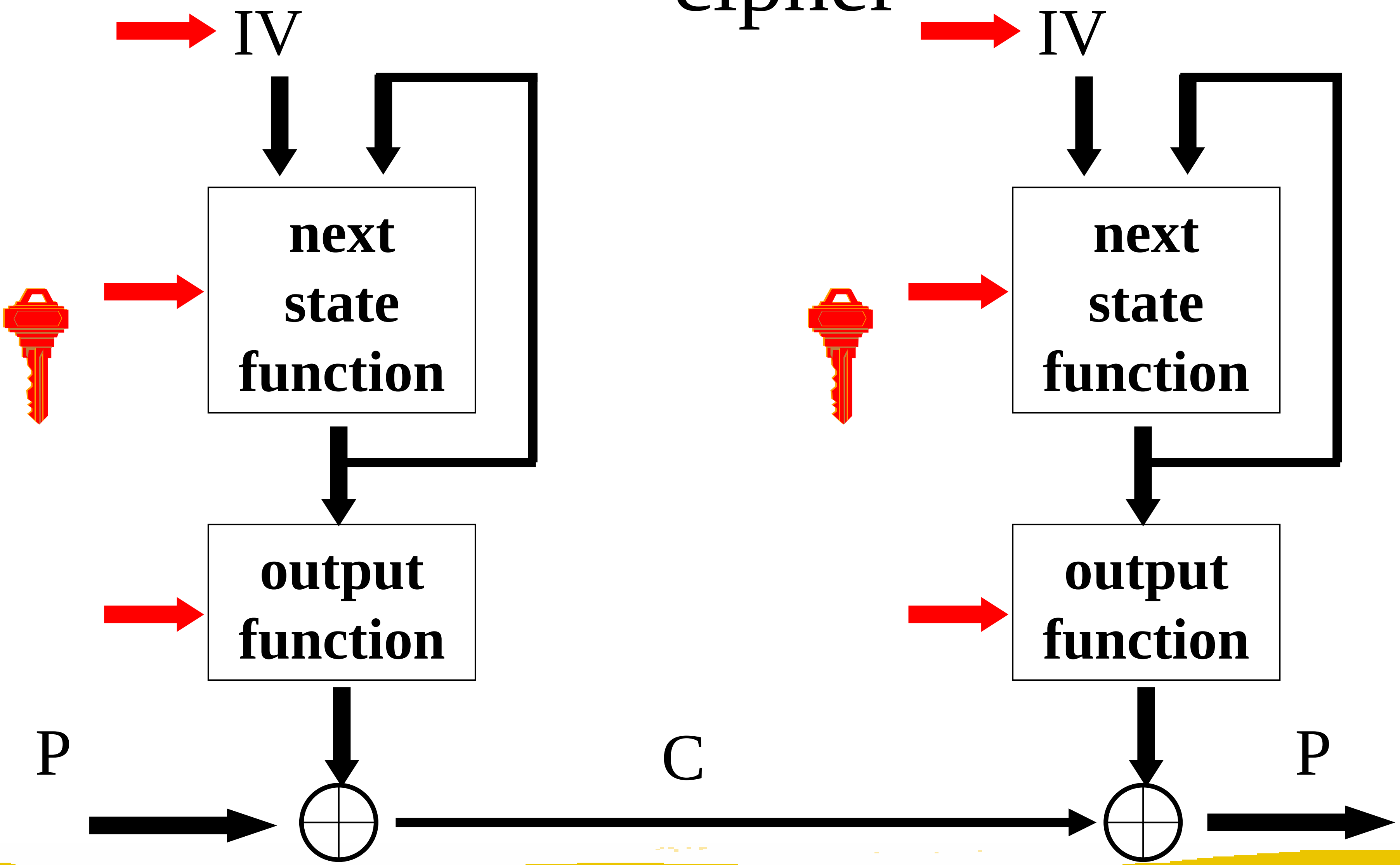
- **information theoretic** security
  - ciphertext only
  - part of ciphertext only
  - noisy version of ciphertext
- **system-based** or practical security
  - also known as “prayer theoretic” security
- **complexity theoretic** security:

  model of computation, definition, proof
  - variant: quantum cryptography

Design of ciphers

- More on this in a week (Sept. 11 / 16)
- For now, the high-level details
  - Symmetric key cryptography
    - Stream ciphers
    - Block ciphers
    - Message authentication codes (MACs)
    - Hash functions
  - Public key cryptography
    - Encryption
    - Digital signatures

Model of a practical stream cipher

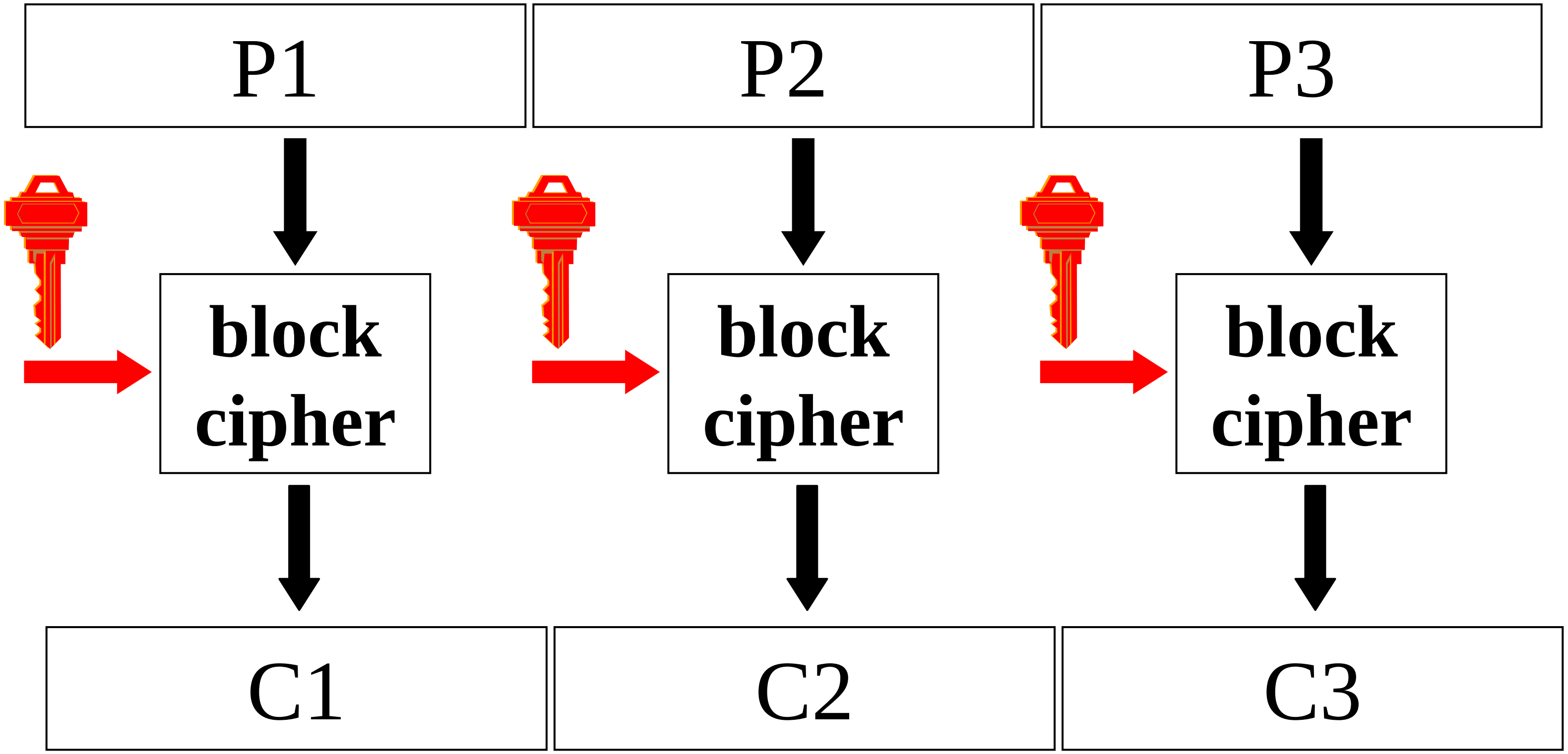


Example stream ciphers

- Bluetooth
- A5 (used in GSM cel phones)
- RC4 (used by most SSL web sites)

- Generally faster than block ciphers
  - Often less secure
  - If you ever reuse a key, the system collapses

Block cipher



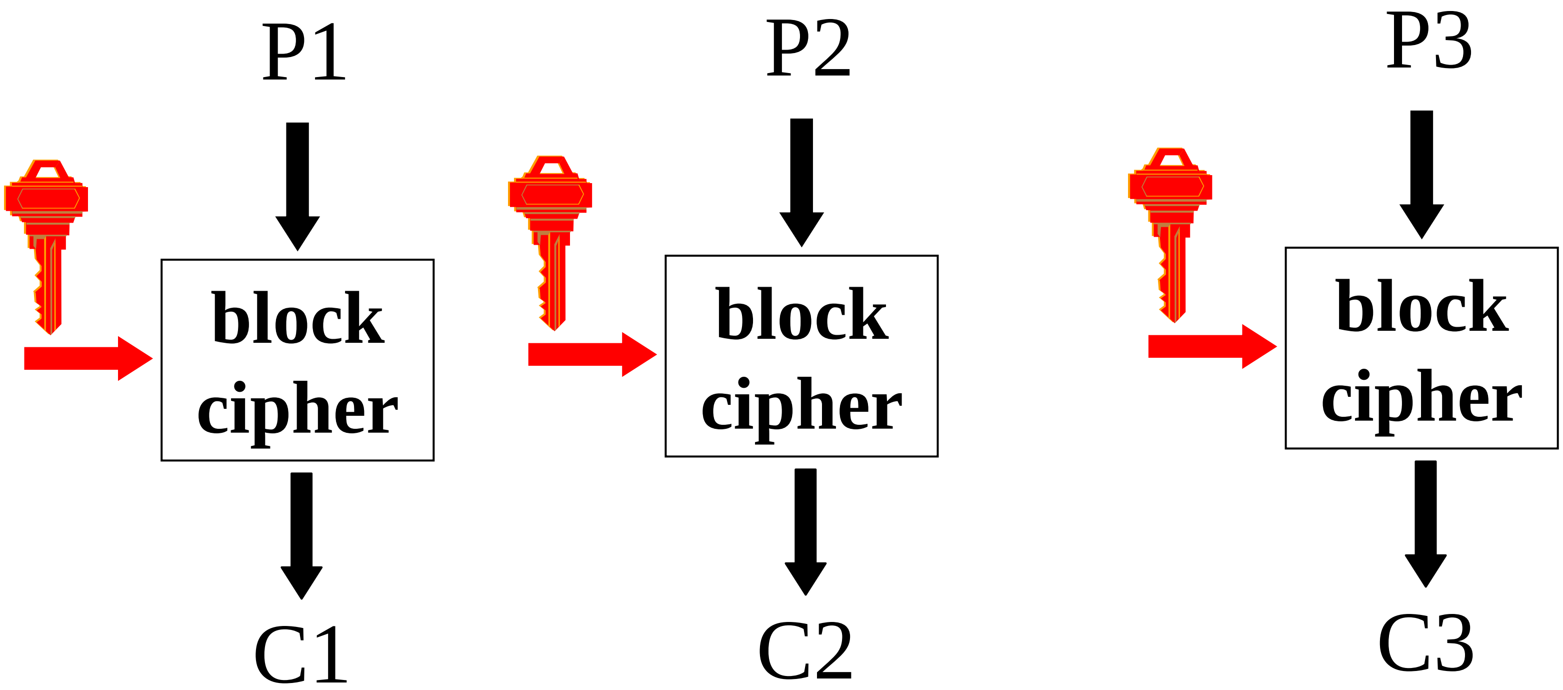
- larger data units: 64…128 bits
- memoryless
- repeat simple operation (round) many times

Example block ciphers

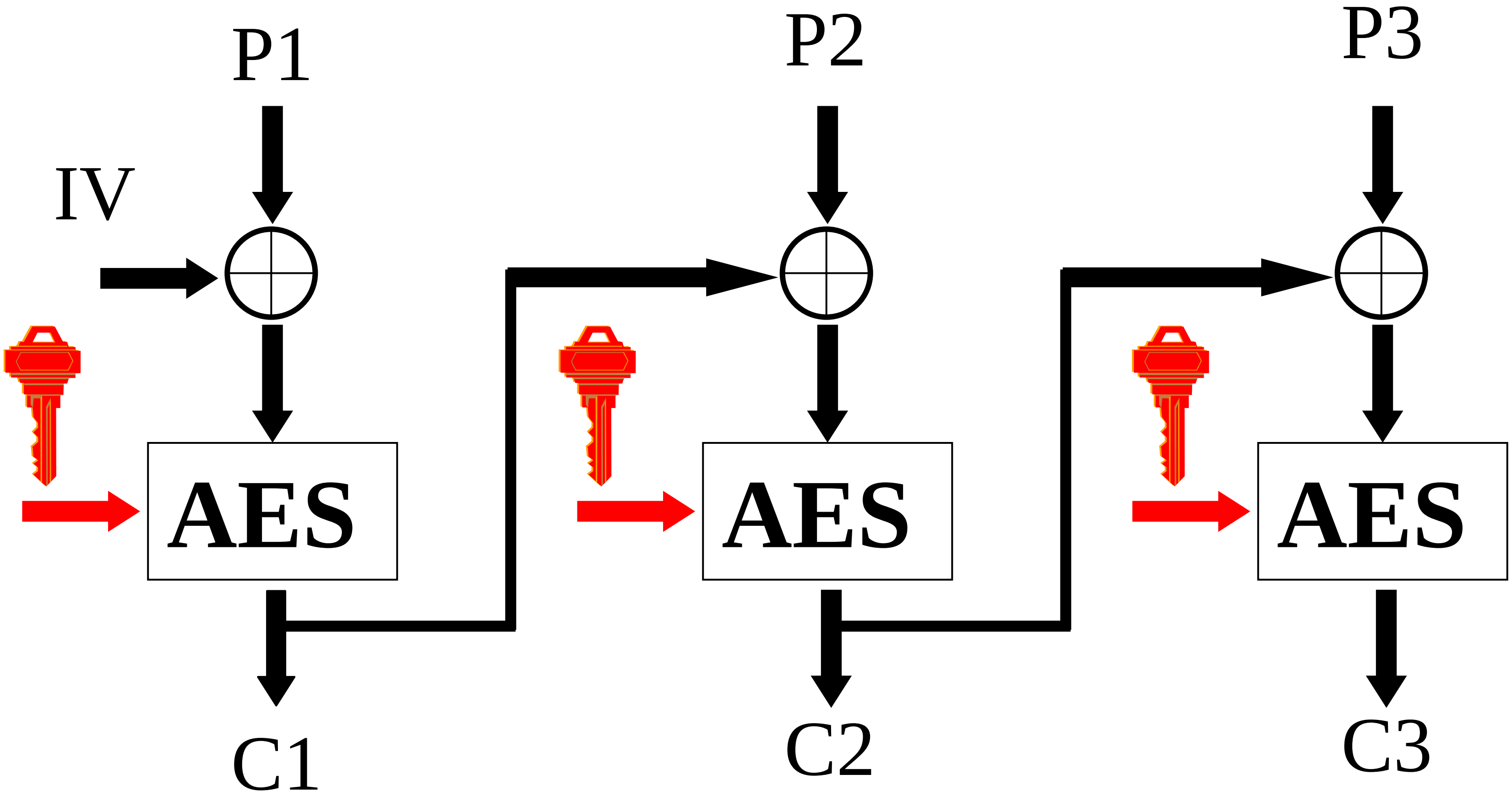
- DES (56-bit), Triple-DES (168-bit)
- AES / Rijndael (several key lengths)
- Many, many others

- Generally slower
- Very versatile: can make stream ciphers, hash functions, many other uses

How NOT to use a block cipher: ECB mode

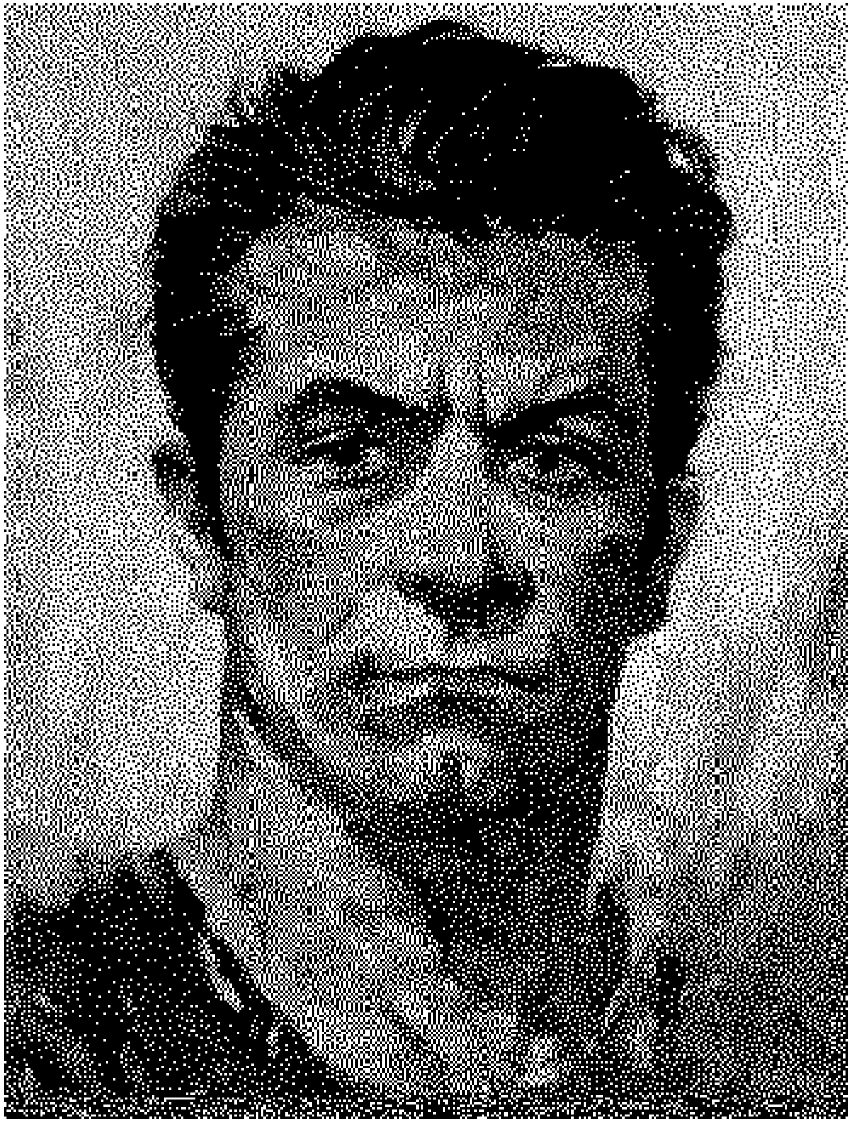


How to use a block cipher: CBC mode

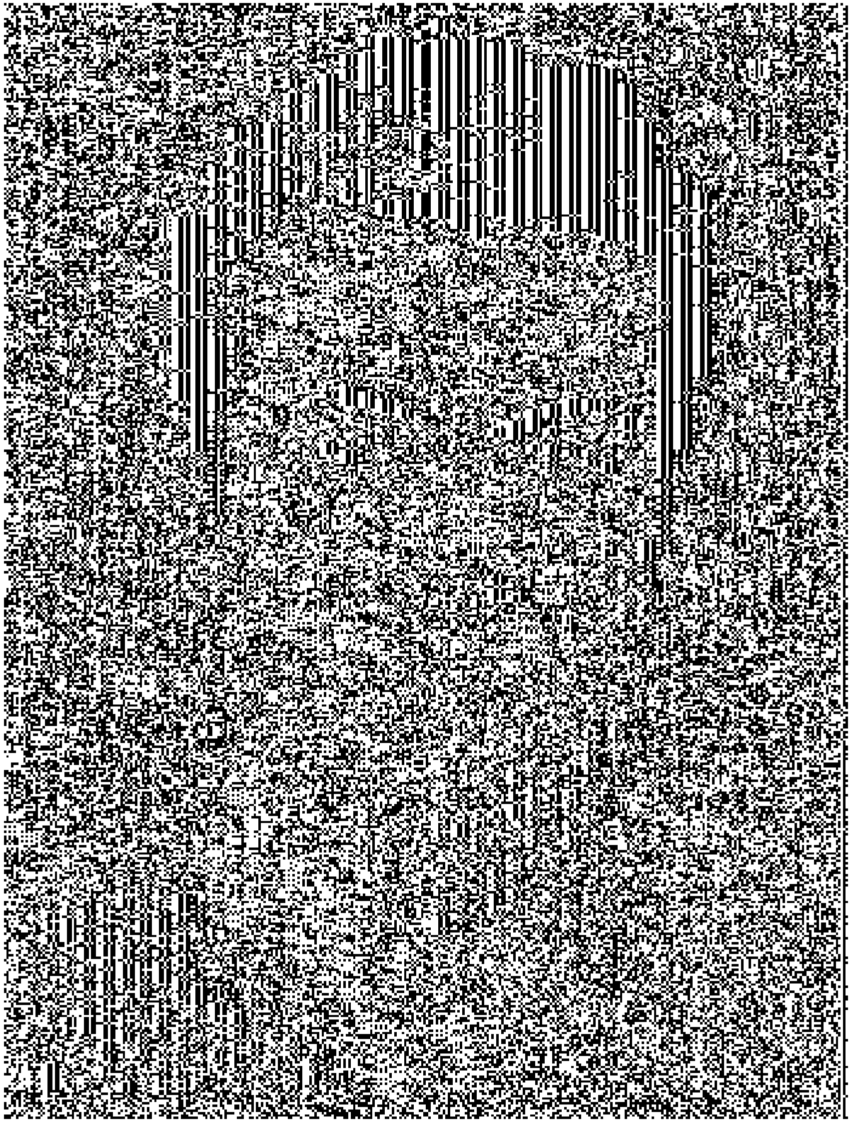


need random IV

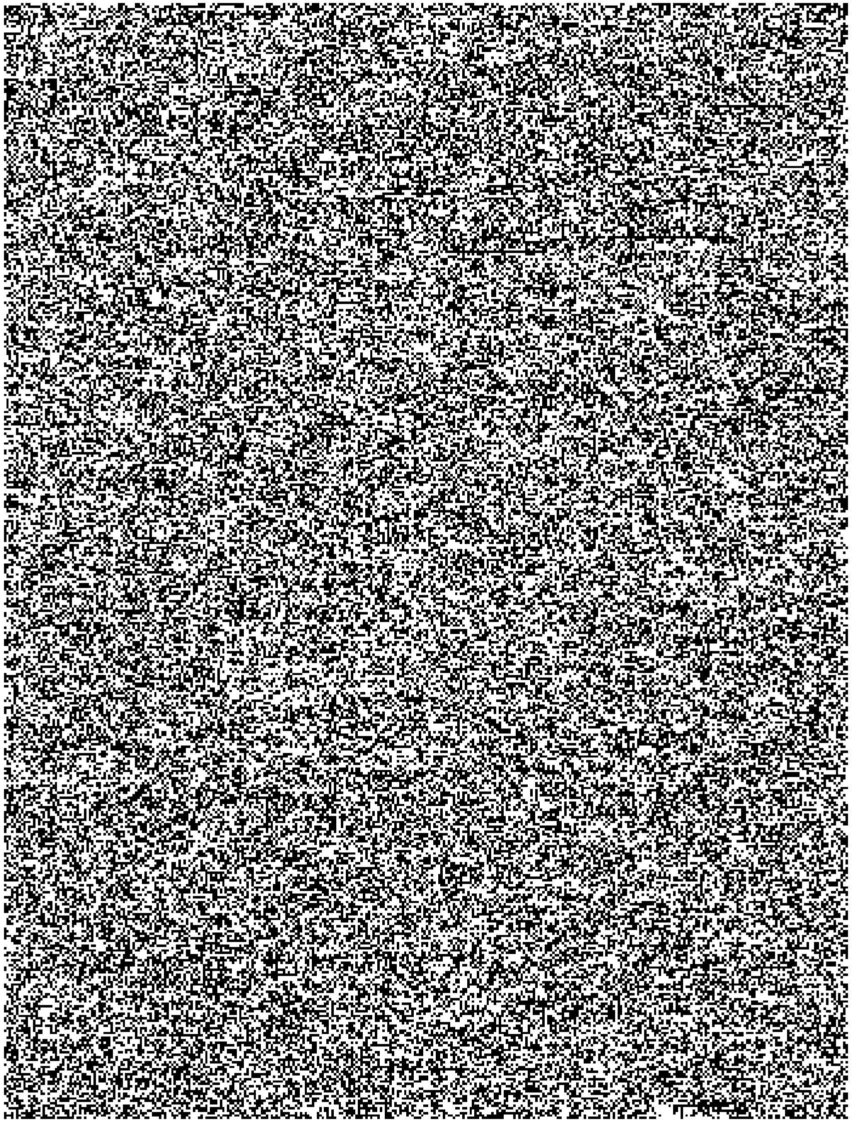
An example plaintext



Encrypted with AES in ECB mode



Encrypted with AES in CBC mode



Symmetric cryptology: data authentication

- the problem
- hash functions without a key
  - MDC: Manipulation Detection Codes
- hash functions with a secret key
  - MAC: Message Authentication Codes

Data authentication: the problem

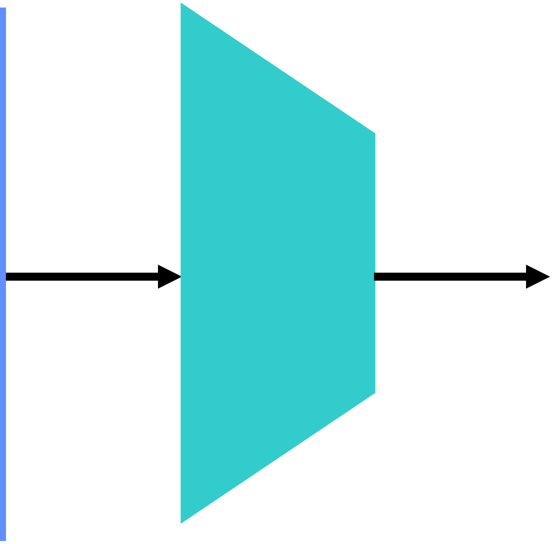
- encryption provides confidentiality:
  - prevents Eve from learning information on the cleartext/plaintext
  - but does not protect against modifications (active eavesdropping)
- Bob wants to know:
  - the **source** of the information (data origin)
  - that the information has not been **modified**
  - (optionally) **timeliness** and **sequence**
- data authentication is typically more complex than data confidentiality

Data authentication: MDC

- MDC (manipulation detection code)
- Protect short hash value rather than long text

- (MD5)
- SHA-1
- SHA-256, -512
- RIPEMD-160

This is an input to a cryptographic hash function. The input is a very long string, that is reduced by the hash function to a string of fixed length. There are additional security conditions: it should be very hard to find an input hashing to a given value (a preimage) or to find two colliding inputs (a collision).



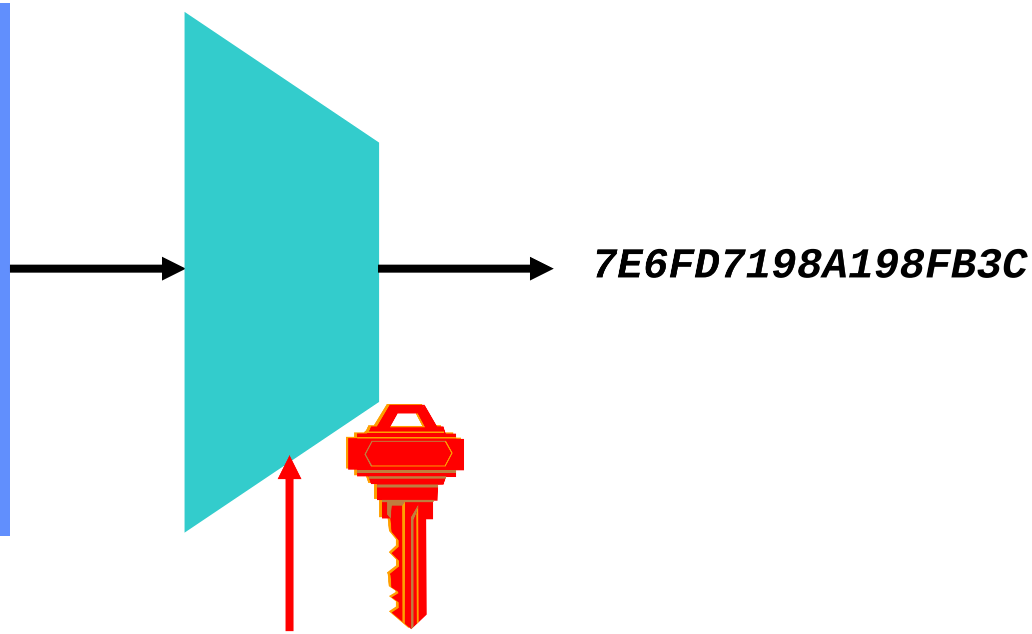
1A3FD4128A198FB3CA345932

Data authentication: MAC

- Replace protection of authenticty of (long) message by protection of secrecy of (short) key
- Add MAC to the plaintext

- CBC-MAC
- HMAC

This is an input to a MAC algorithm. The input is a very long string, that is reduced by the hash function to a string of fixed length. There are additional security conditions: it should be very hard for someone who does not know the secret key to compute the hash function on a new input.



MAC algorithms