Security

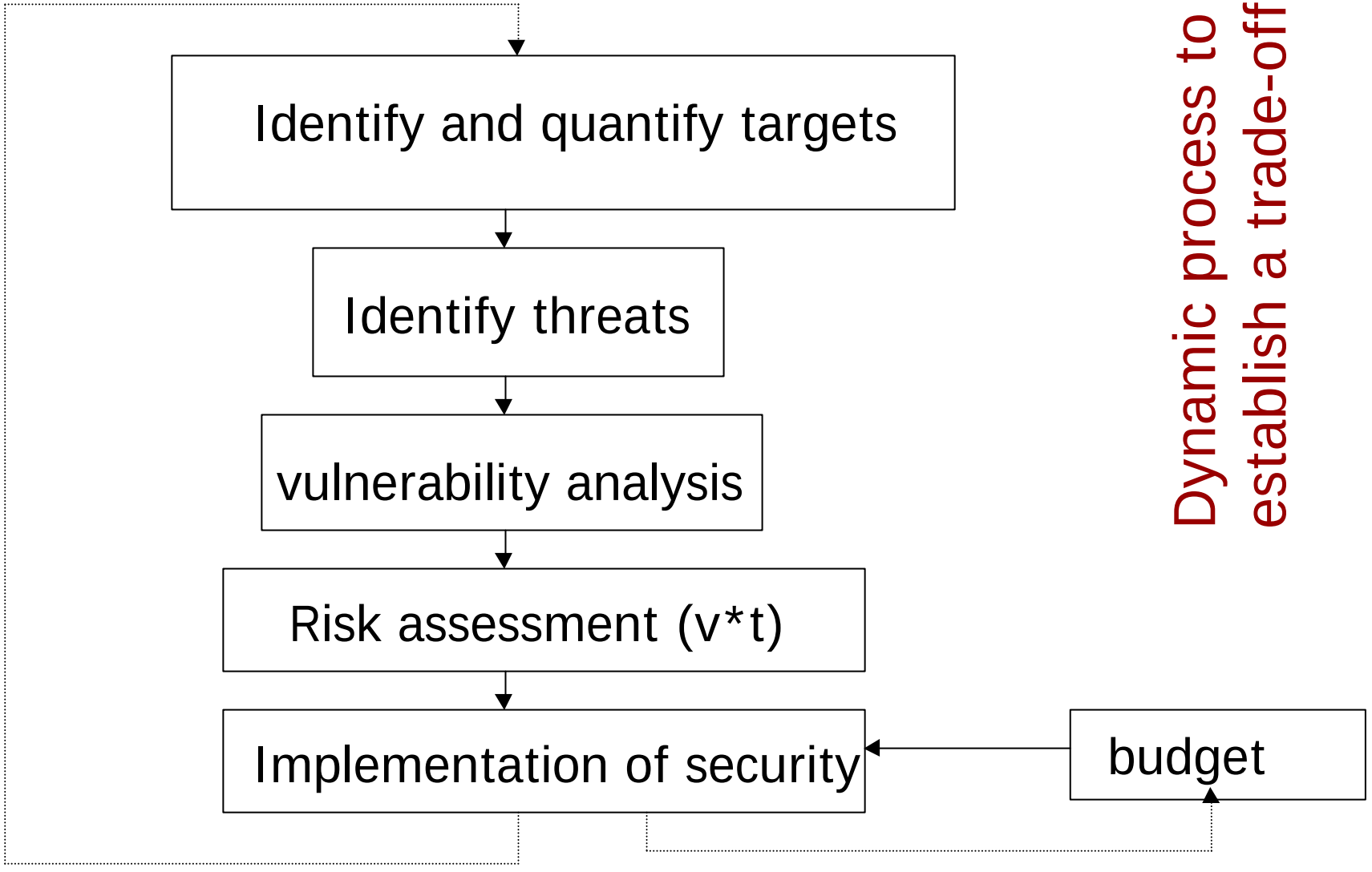
crispo@cs.vu.nl

text book: Network Security, second edition,
C. Kaufman, R. Perlman and M. Specimer,
Prentice Hall ed.

slides at www.cs.vu.nl/~crispo/teaching

classes: Tuesday 14.45-16.30 room M143

Risk Analysis



Implementation of security

- Technical ..what we cover in this course

- Documentation $\rightarrow$ security policies
  - principles and goals
  - application domain
  - compliance to laws and standards
  - personnel roles and responsibilities
  - description of technical mechanisms and their maintenance and management

Basic security properties

- Confidentiality: to prevent unauthorised disclosure of the information
- Integrity: to prevent unauthorised modification of the information
- Authentication: to prove the claimed identity can be Data or Entity authentication
- Availability: to guarantee access to information

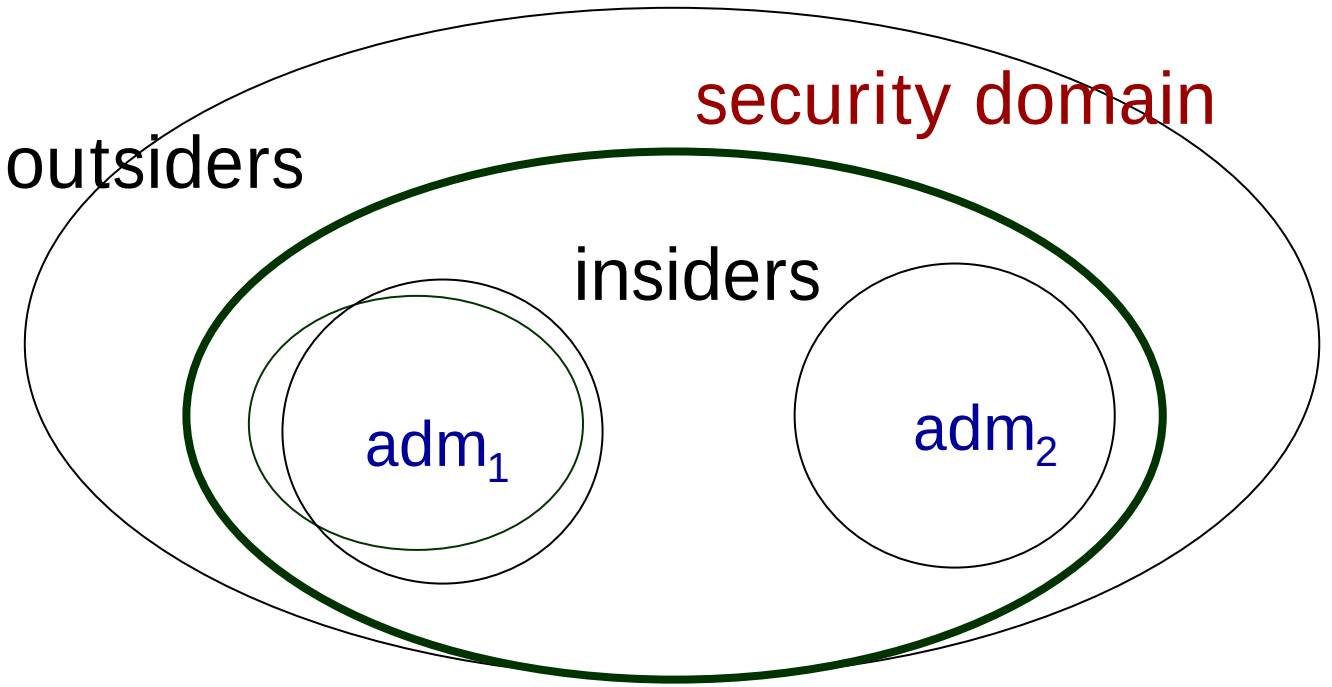
Auxiliary security properties

- Non repudiation: to prevent false denial of performed actions
- Authorisation: ”what Alice can do”
- Auditing: to securely record evidence of performed actions
- Fault-tolerance: ability to provide some degree of service after failures or attacks
- Disaster Recovery: ability to recover a safe state
- Key-recovery, key-escrow, ...

Security mechanisms

- Encryption/Decryption
- Digital signatures
- Message authentication code
- Hash functions
- Key exchange
- Key distribution
- Time stamping

Types of attacker



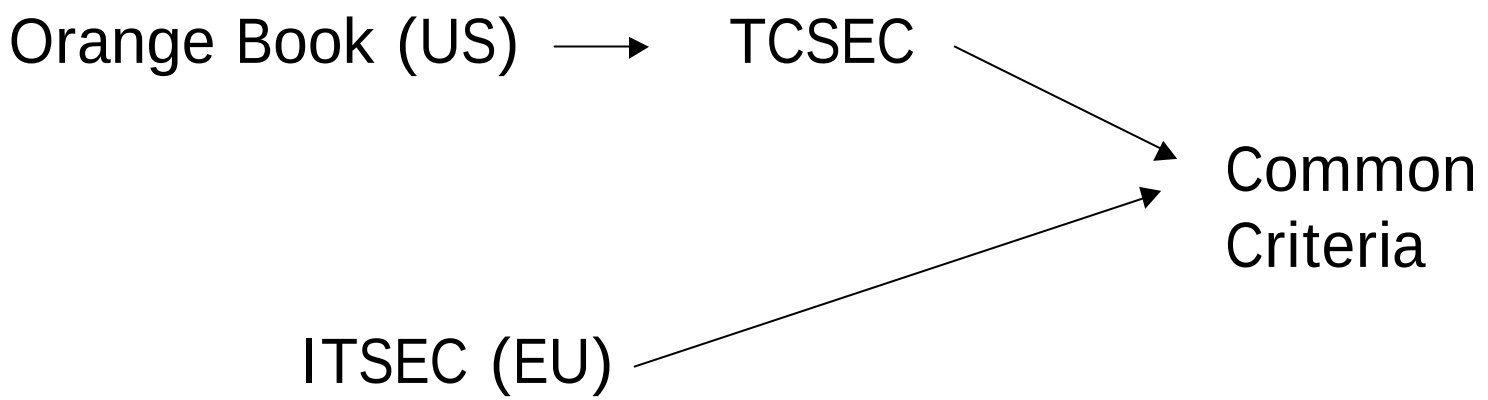
Types of attack

- Passive: the attacker can only read any information
  - Tempest

- Active: the attacker can read, modify, generate, destroy any information

Assurance

- Assurance: confidence that a system meets its security objectives



Orange Book security levels

D	Minimal protection
C1	Discretionary security protection
C2	Controlled access protection
B1	Labeled security protection
B2	Structured Protection
B3	Security Domains
A1	Verified design

Malicious Software

- Viruses
- Worms
- Trojan Horses

- Trapdoor
- Logic bomb
- Zombie

Virus

original program

inst i

inst i+1

inst i+2

inst i+3

....

inst n

attacked program

inst i

inst i+1

x jump k

m inst i+3

.....

inst n

k v_inst 1

copy itself

damage

v_inst end

insti+2

jump m

Antivirus

- Detection rather than prevention
- Pattern matching
- Polymorphic virus
- Executable data → mail attachment, macro

Cryptography

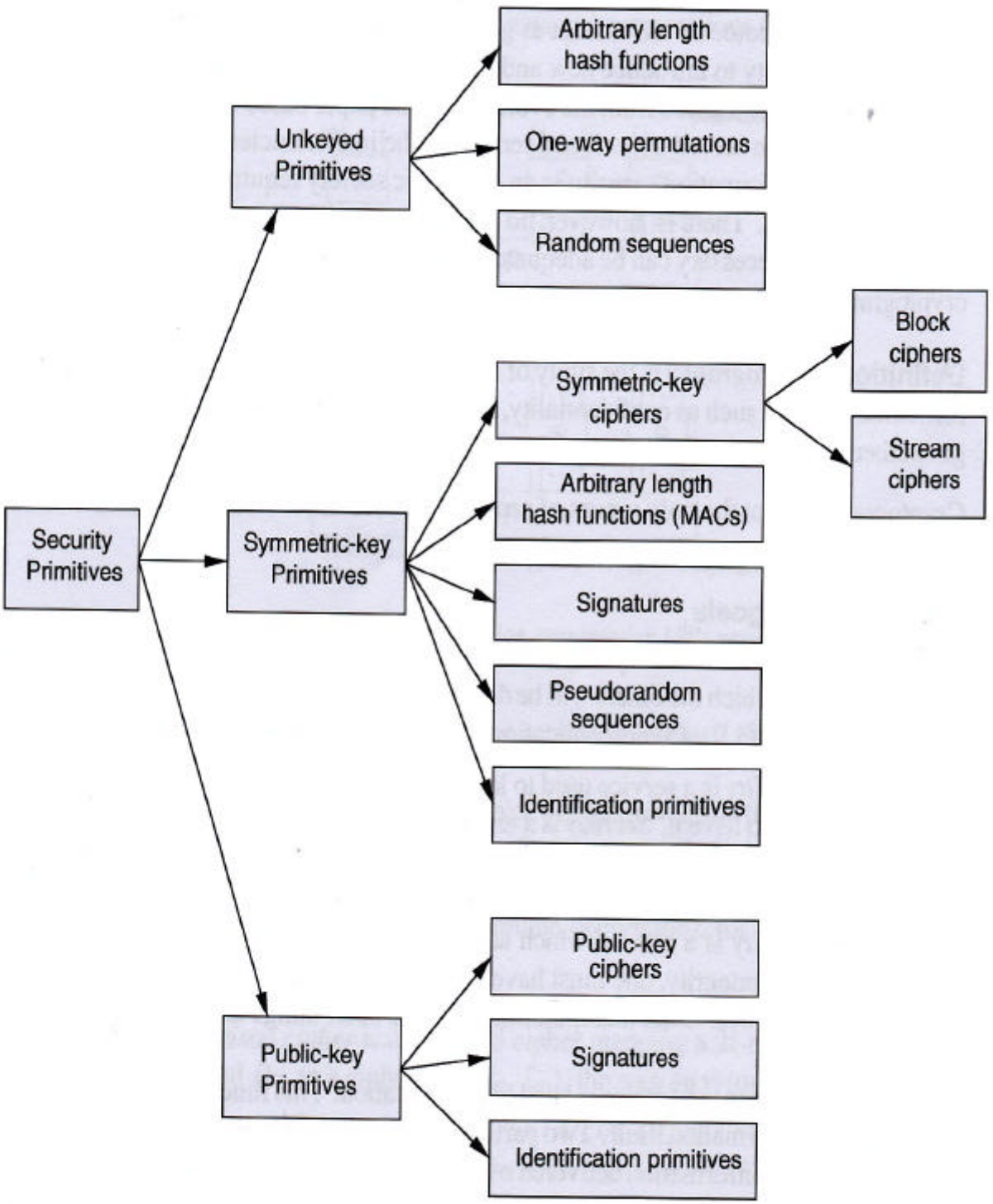


Figure 1.1: *A taxonomy of cryptographic primitives.*

Encryption and Decryption

M=message space, *C*=ciphertext space

K=key space

e∈*K* ® bijection *Ee* :*M* ® *C* encryption function

d ∈*K* ® *bijection Dd*:*C* ®*M* decryption function

Encryption and Decryption

$\{E\mathrm{e}: \mathrm{e} \in K\}$ and $\{D\mathrm{d}: \mathrm{d} \in K\}$

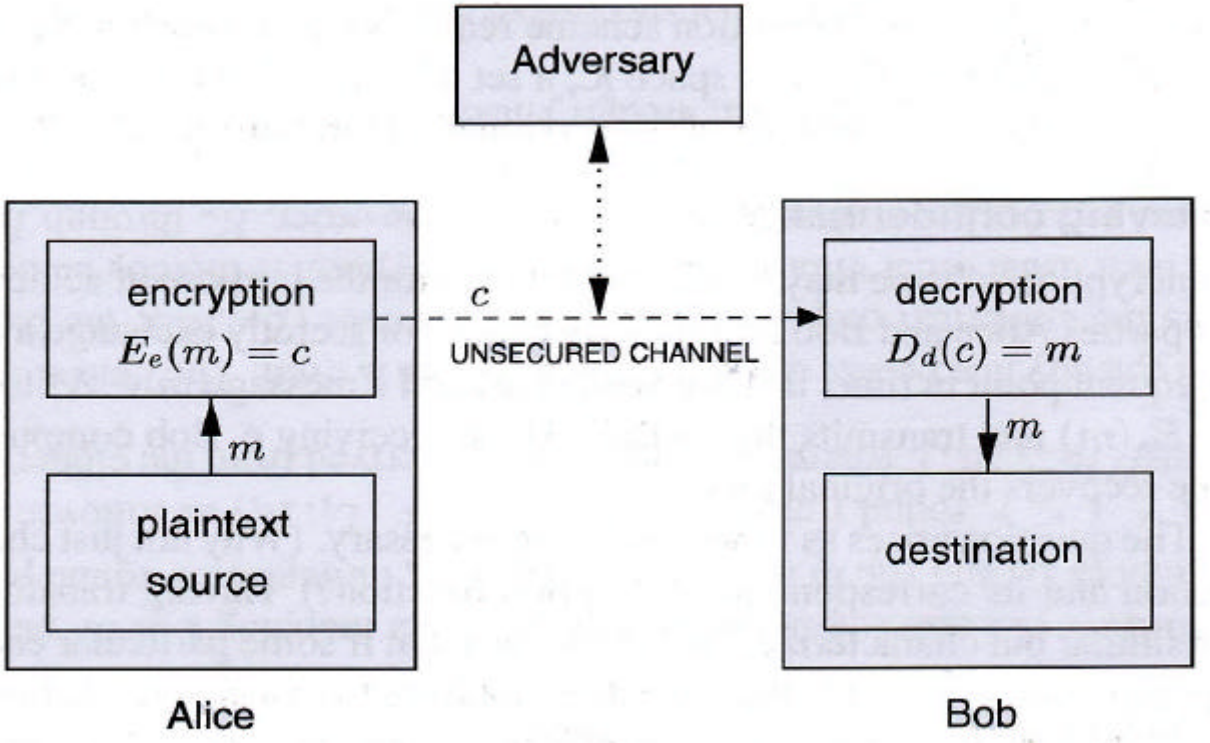
For each $\mathrm{e} \in K$ there is a unique $\mathrm{d} \in K$:

$$D\mathrm{d} = 1/E\mathrm{e} \approx D\mathrm{d}(E\mathrm{e}(\mathrm{m})) = \mathrm{m}$$

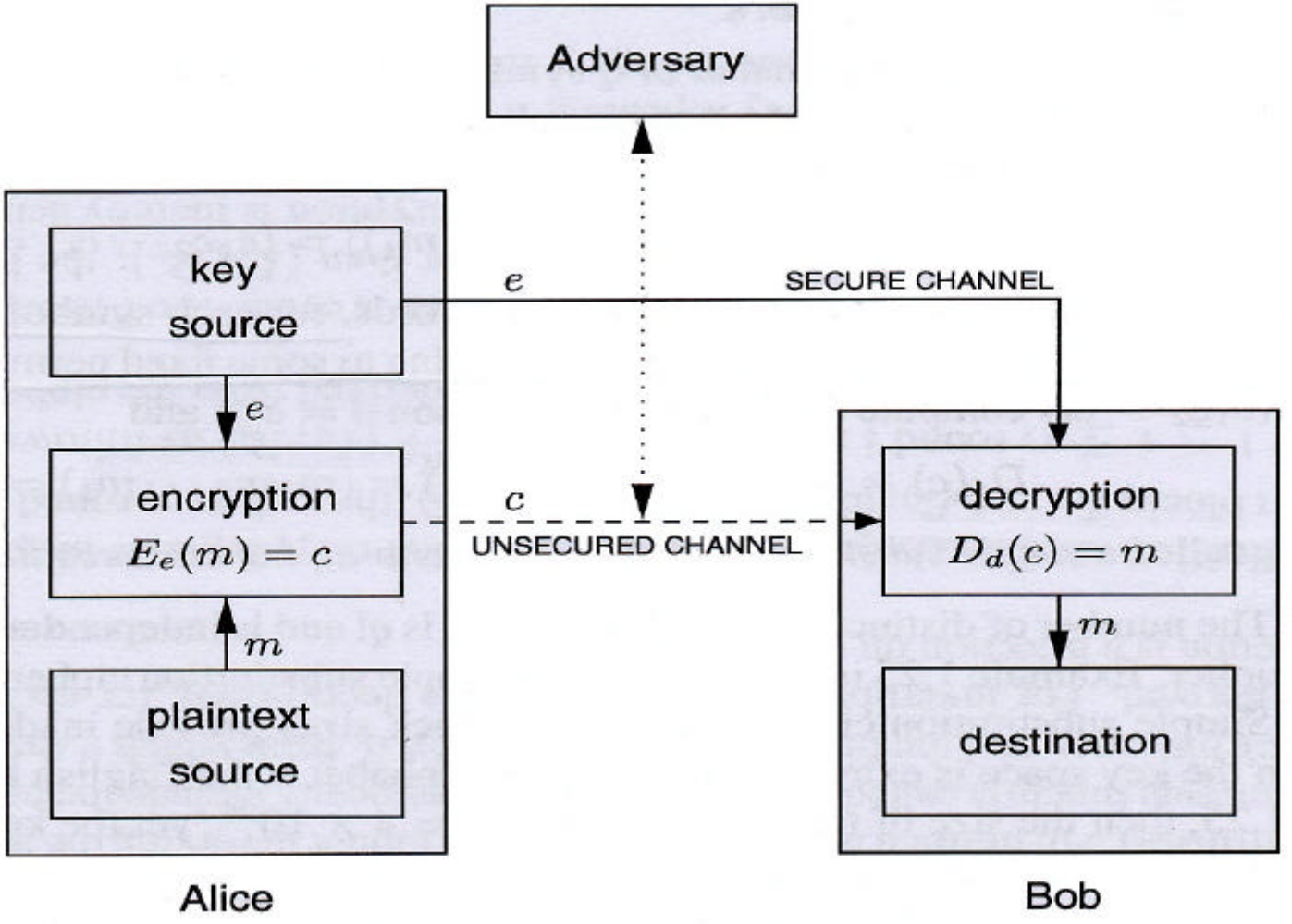
(e,d) key pair e=d symmetric schemes

e≠d asymmetric schemes

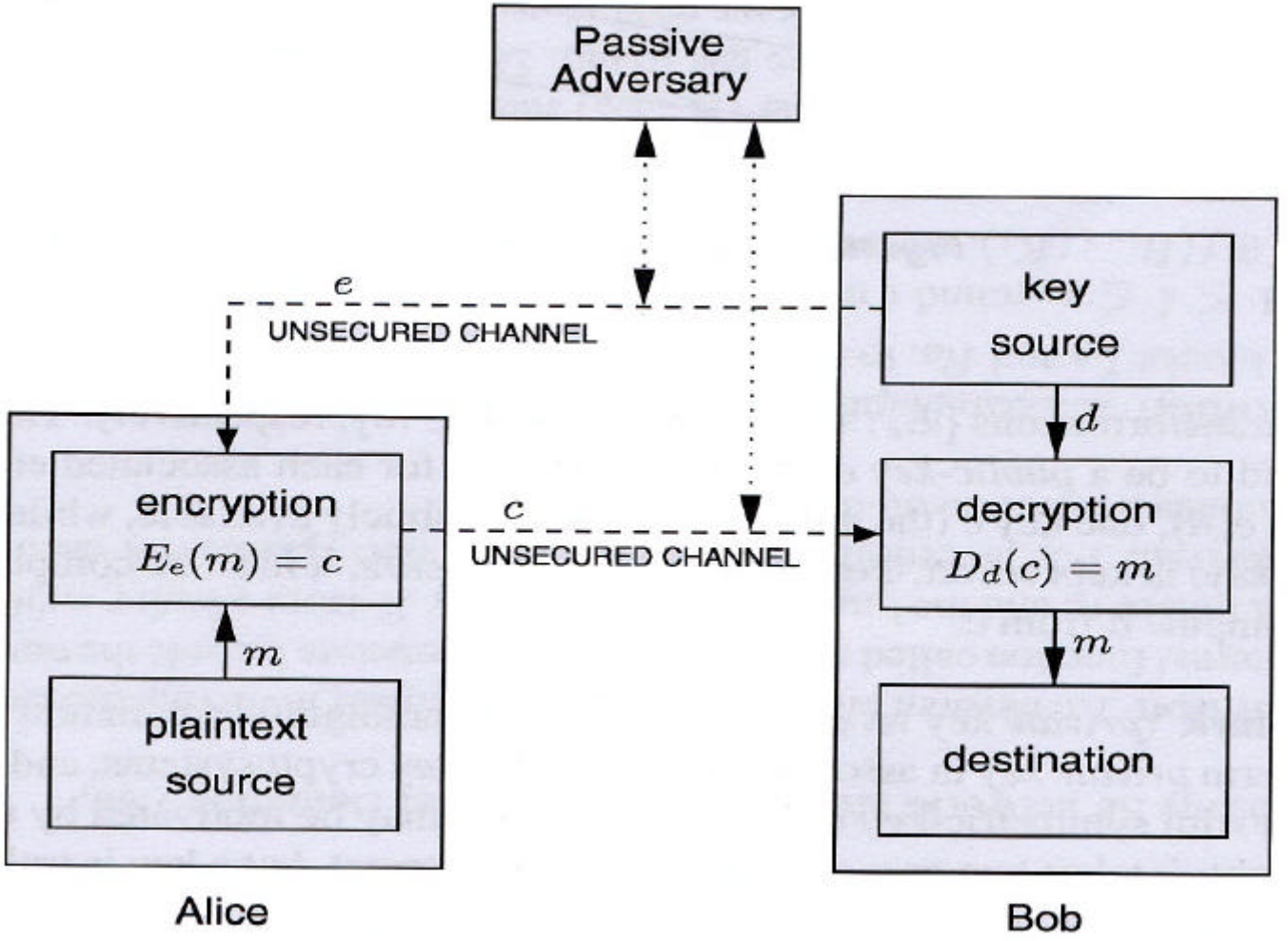
Encryption scheme



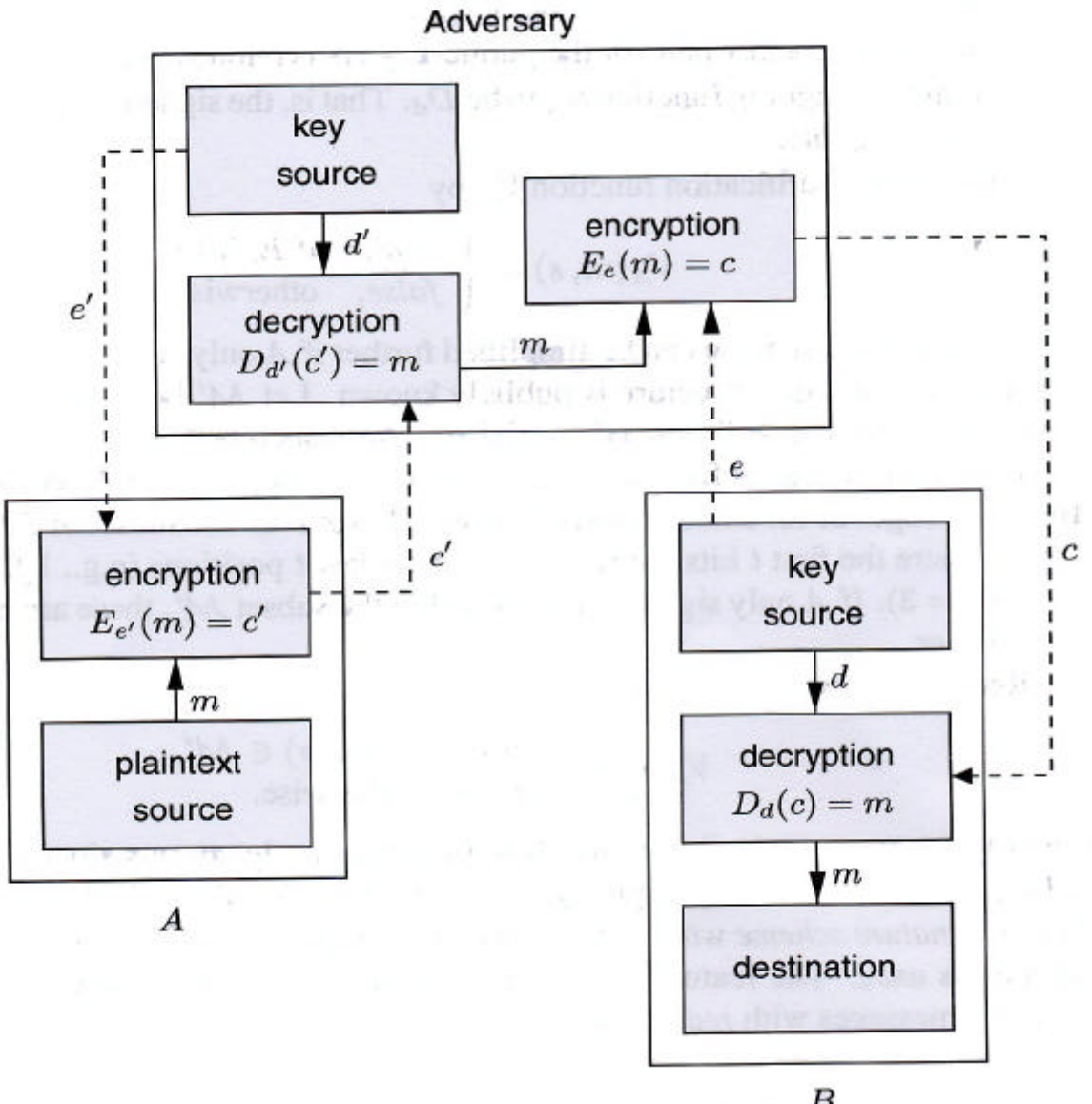
Symmetric key encryption



Asymmetric key encryption

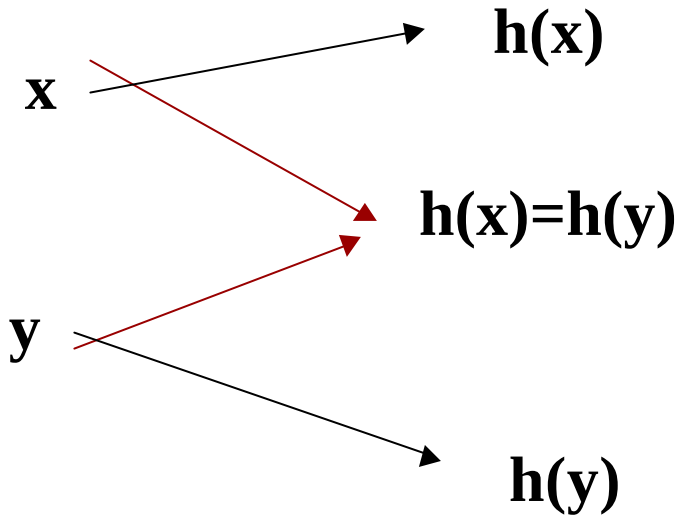


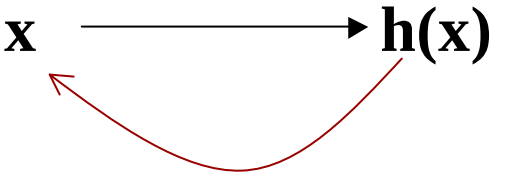
Asymmetric key encryption



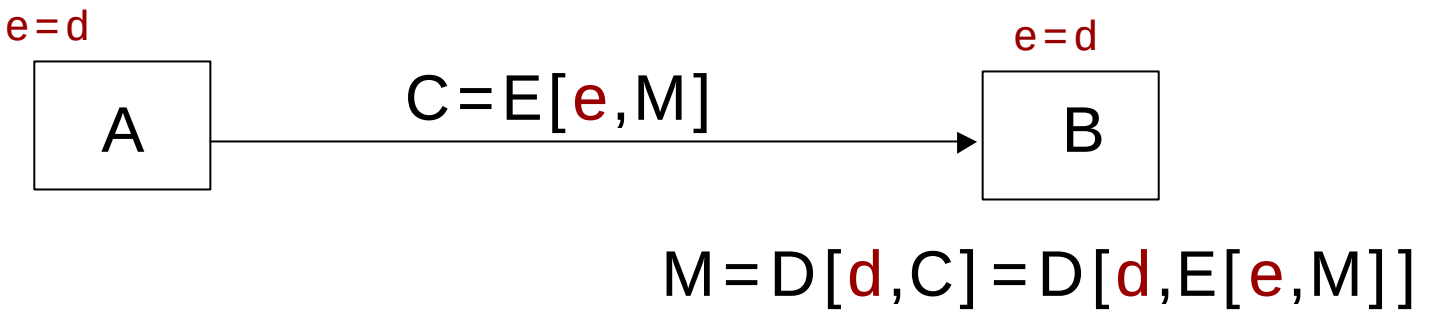
Hash Functions

- One-way functions
- Hash function mapping bs of arbitrary length to bs of fixed length



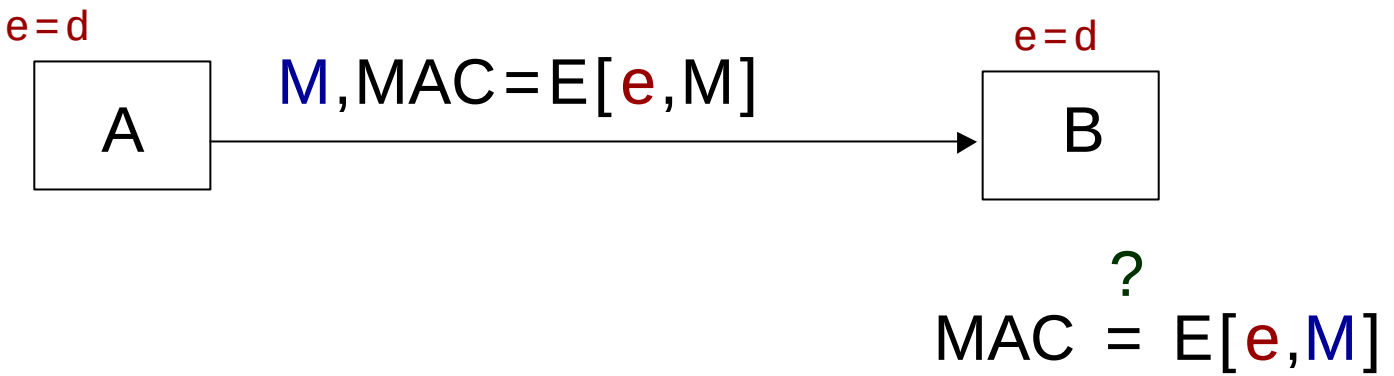


Confidentiality with SK



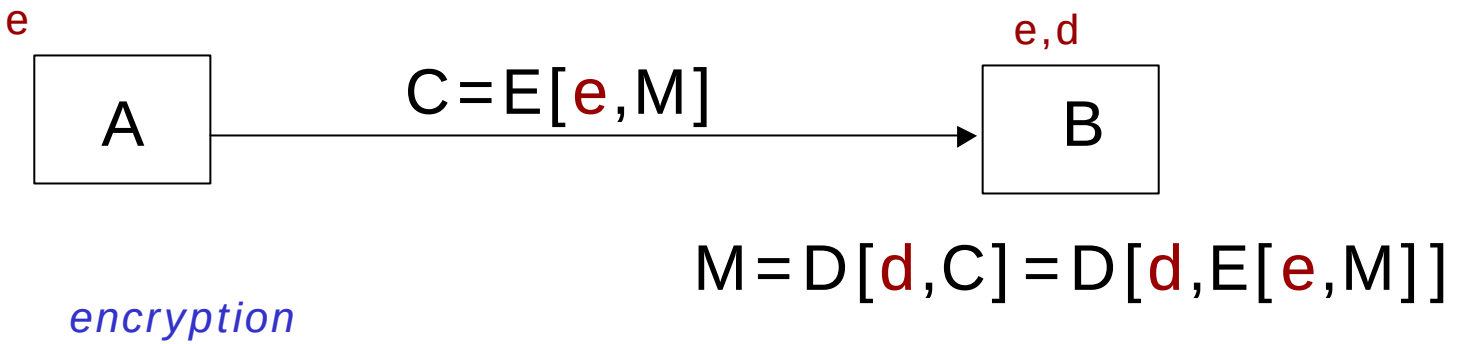
Encryption/decryption

Integrity with SK

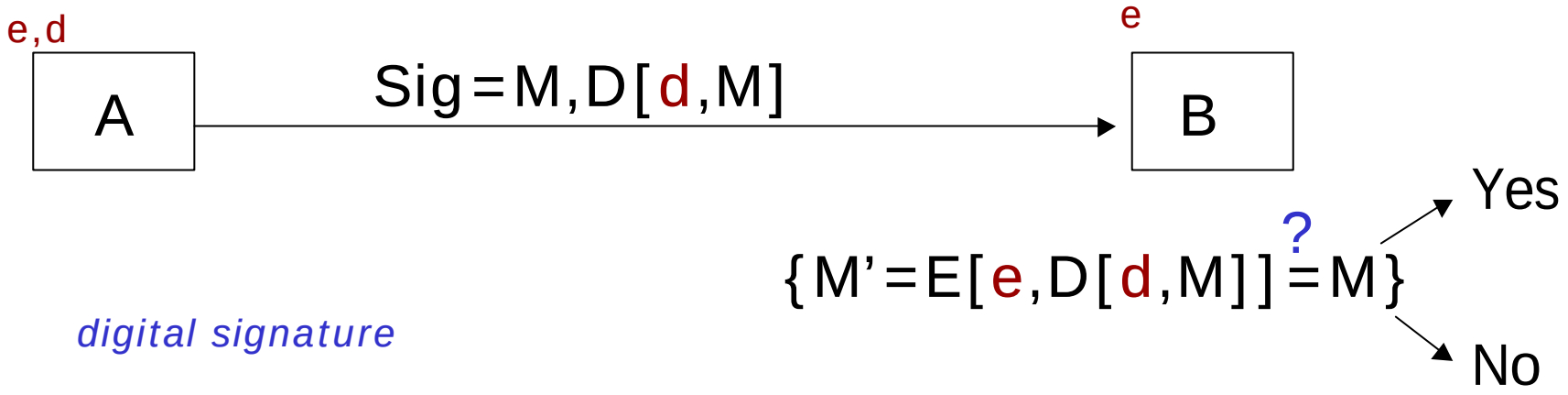


MAC=message authentication code

Confidentiality with AK



Integrity with AK



digital signature

ass: Dd(Ee)≈Ee(Dd)

Digital Signature

- Sig guarantees that only that d can have been used $\rightarrow$ *msg authentication*
- if d $\leftrightarrow$ entity $\rightarrow$ *entity authentication*
- if entity $\leftrightarrow$ user $\rightarrow$ *user authentication*
- if *other conditions* are met a digital signature can be built

Randomness

1 bit input $\rightarrow$ half bits of the output

N randomly chosen input $\rightarrow$ any particular bit of the output will be on half the time

Kerchoffs' principles

- Theoretically unbreakable, or at least unbreakable in practice
- Ciphertext transmitted over unsecure channel
- Security of the scheme should reside only in the chosen key

Type of attacks

- Passive: the attacker can only read any information

  confidentiality

- Active: the attacker can read, modify, generate, destroy any information

  integrity,authenticity and confidentiality

Attacks on encryption schemes

- Ciphertext only
- Known-plaintext
- Chosen-plaintext
- Adaptive chosen-plaintext
- Chosen-ciphertext
- Adaptive chosen-ciphertext

Security strength

- Unconditional security (Otp)
- Complexity-theoretic security
- Provable security
- Computational security
- Ad hoc security