Lesson 2 – Security Concepts

Information systems security is the ability to

provide the services required *by the user community while simultaneously* ***preventing unauthorized use*** *of system resources.*

Security review

- **Objective: protect information**
  - Confidentiality
  - Integrity
  - Availability
- **Provided by:**
  - having a plan (risk assessment, policy)
  - educating users/programmers
  - Secure applications and tools -- hashing, signing, encryption

Security goals – CIA model

- **Confidentiality**
  - Includes corporate information, such as Accounting, Production, Research, Sales and Marketing secrets
  - Includes access information, such as passwords
- **Integrity**
  - Has the data been manipulated ?
  - Is the system in the desired state or has someone changed it ?
- **Availability**
  - Are services and data available when needed
  - What downtimes are tolerated

Assets (what you are trying to protect)

- Logical resources
  - Information
  - Electronic money
  - Personal data
  - Credit card data
  - Electronic goods (software, music, pictures, tickets, etc.)
- Physical resources
  - Hardware
  - Buildings
  - People
  - Physical money
  - Goods (food, clothes, cars, etc.)

Threats or Attacks

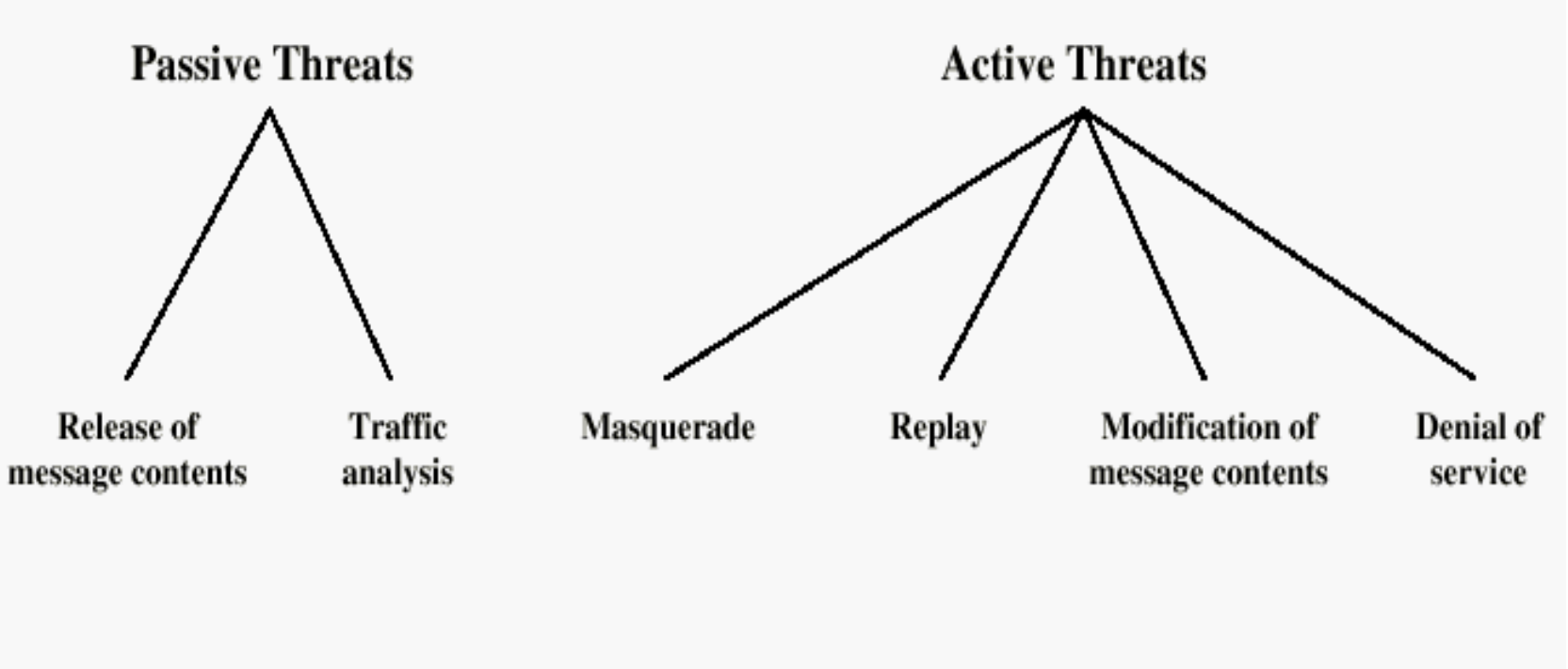
Threat : a potential for violation of security

Attack: a violation of security

- Intentional
  - Attack by intelligent agent
- Accidental
  - Errors, omissions, malfunctions, natural disaster

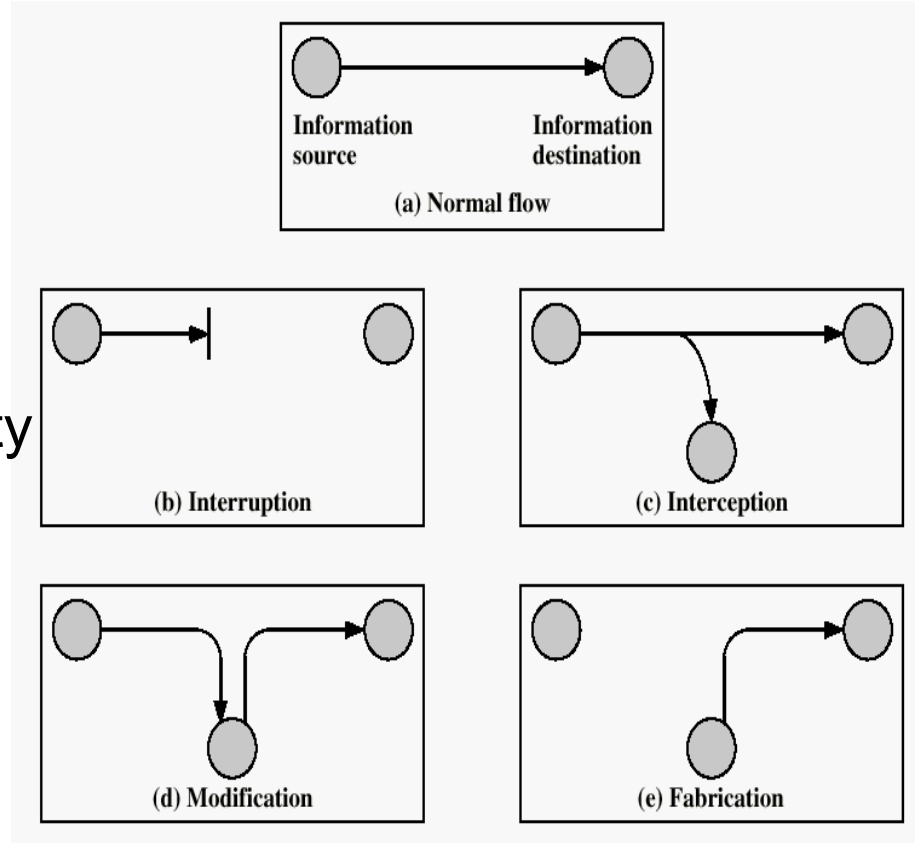
- Passive
  - No change to the state of the system
- Active
  - Change the state of the system

Some passive and active threats



Security Attacks

- Interruption:
  - This is an attack on availability
- Interception:
  - This is an attack on confidentiality
- Modification:
  - This is an attack on integrity
- Fabrication:
  - This is an attack on authenticity



Attacks, Services and Mechanisms

- Security Attack:
  - Any action that compromises the security of information.
- Security Mechanism:
  - A mechanism that is designed to detect, prevent, or recover from a security attack.
- Security Service:
  - A service that enhances the security of data processing systems and information transfers. A security service makes use of one or more security mechanisms.

Thought Experiment (from Dr. Bill Young)

- Imagine you have a friend who lives in some foreign country where the secret police spy on everyone and everything, and you want to send a valuable object to this friend. You have a strongbox big enough to hold the object. The box has a lock ring that can accommodate several locks. But your friend does not have the key to any lock that you have.
- You can't send a key in the mail because the secret police will intercept and copy it. You can't leave the box unlocked, because the object is too valuable. Ideally, you'd lock the object in the box and mail it to your friend, so that he can open it, but the secret police can't.
- How could you do it?

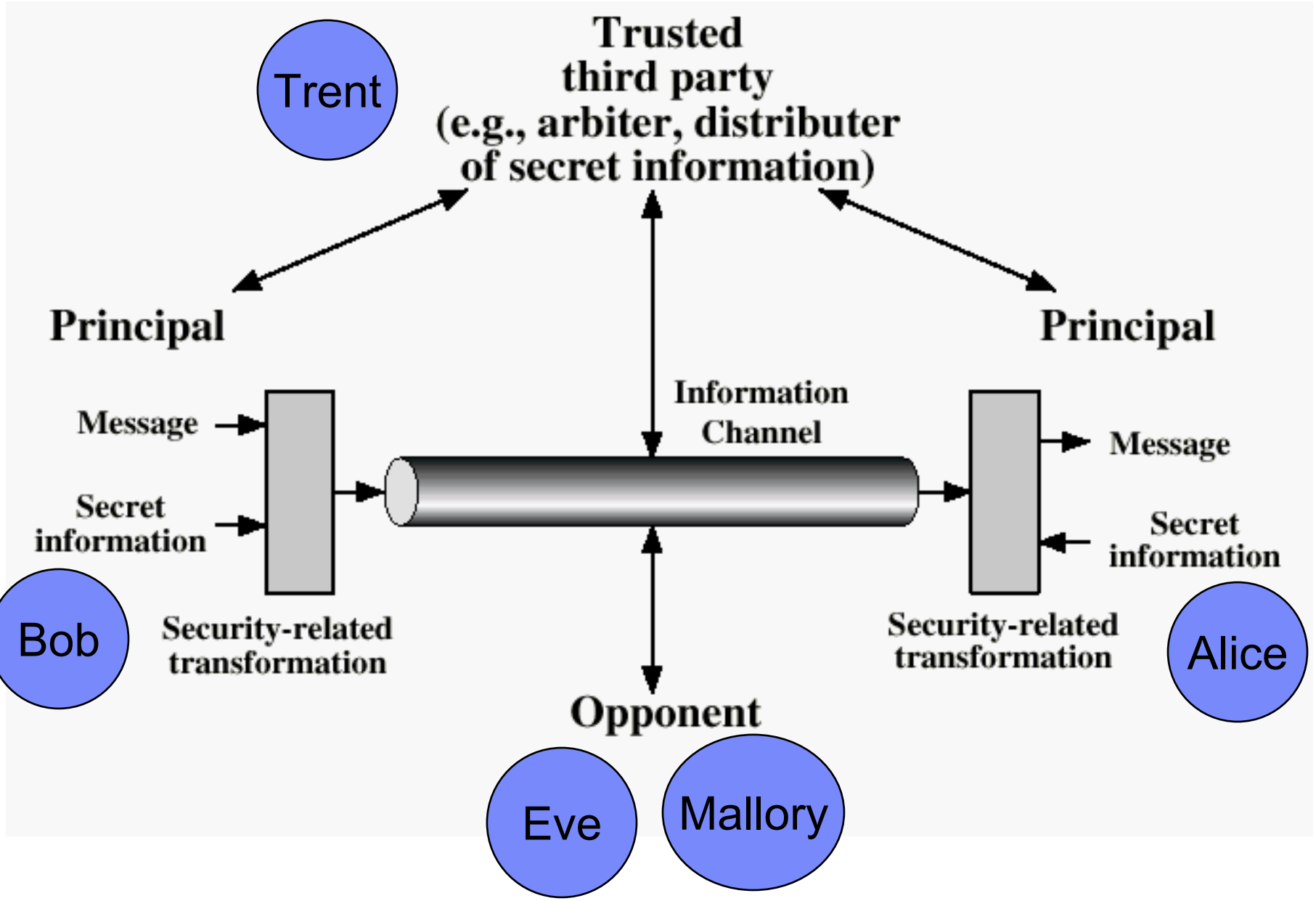
Thought Experiment

- The remote control used to unlock the doors of cars manufactured up to the mid-1990s used an embedded password that is transmitted when the user press the open door button. These primitive remote controls just broadcast their 16-bit serial number, which also acts as the password. The car is programmed to open the door when a particular password is received.
- Can be represented as:
  - user -> car : password
- How many passwords are in this system?
- Can you design an attack to this mechanism?
- How can you improve this mechanism?

Break

Cryptographic or security protocols

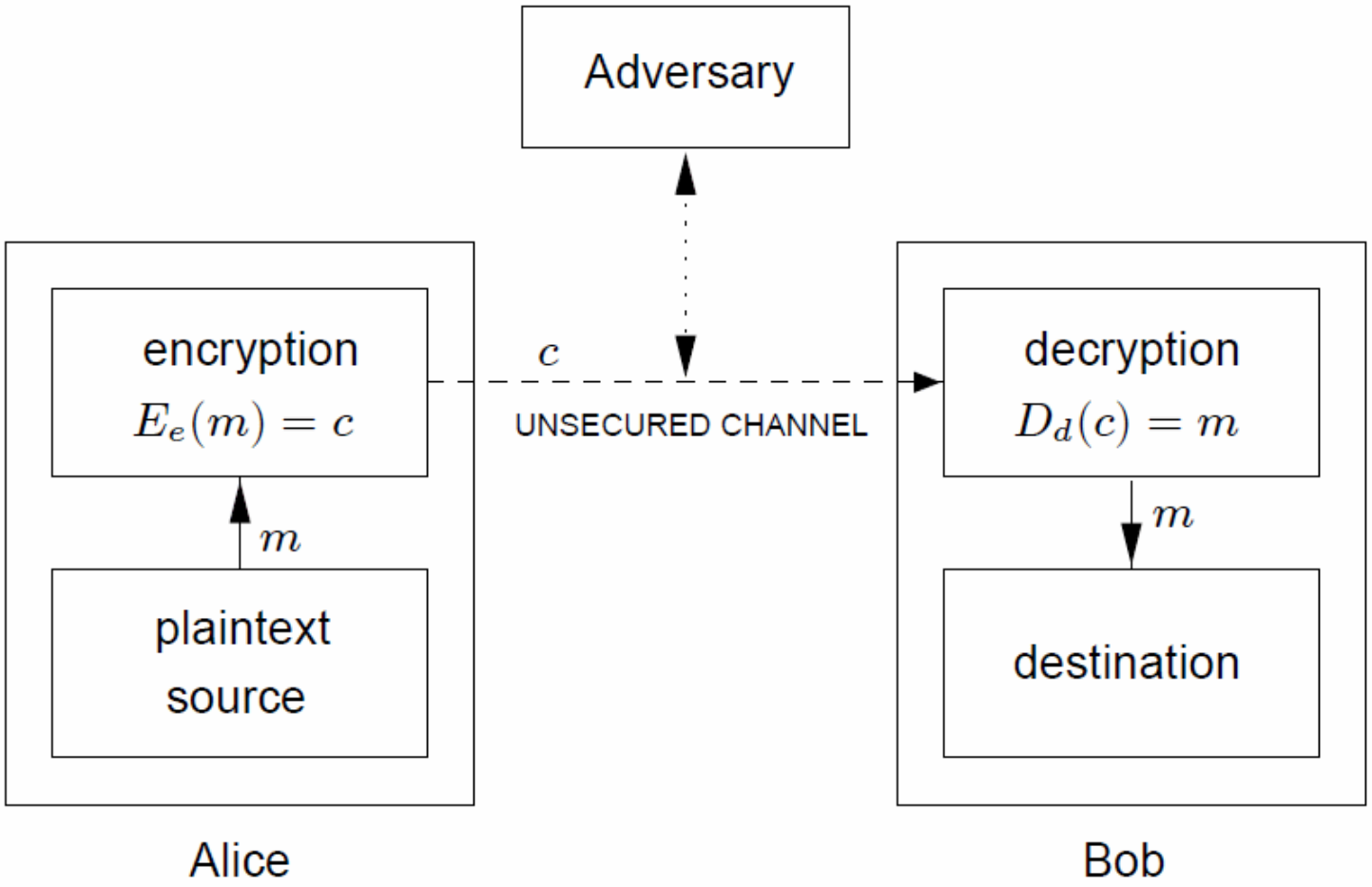
- Designed to secure communication
  - A series of steps
  - Involves two or more parties
  - Designed to accomplish a task
- Uses cryptographic primitives (e.g. encryption, hash function, etc.)


Trent
Trusted
third party
(e.g., arbiter, distributer
of secret information)
Principal
Principal
Information
Channel
Message
Secret
information
Message
Secret
information
Bob
Security-related
transformation
Security-related
transformation
Alice
Opponent
Eve
Mallory

Some goals of cryptographic protocols

- Authentication
- Key agreement or establishment
- Symmetric encryption and message authentication
- Secured application-level data transport
- Non-repudiation

Two-party communication using encryption



Handbook of Applied Cryptography by A. Menezes, P. van Oorschot and S. Vanstone. Pg 13

God protocol properties

- Secrecy:
  - May an intruder learn some secret message between two honest participants?
- Authentication:
  - Is the agent Alice really talking to Bob?
- Fairness:
  - Alice and Bob want to sign a contract. Alice initiates the protocol. May Bob obtain some advantage?
- Non-repudiation:
  - Alice sends a message to Bob. Alice cannot later deny having sent this message. Bob cannot deny having received the message

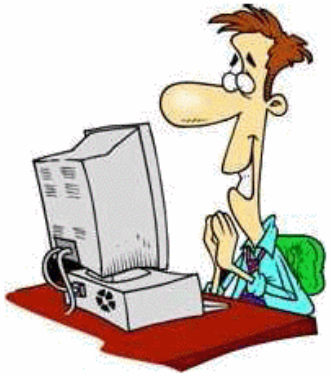
For a protocol to work

- Everyone involved must
  - Know the protocol
  - Agree to follow it
- The protocol must be
  - Unambiguous
  - Complete

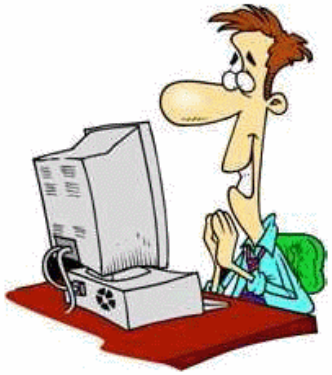
Two main types of cryptographic attacks

- Breaking the encryption
  - Cryptanalysis
- Logical attacks
  - Known-key attack:
    - Attacker gains some keys used previously and then uses this info to attack the protocol and possibly determine new keys
  - Replay:
    - Attacker records a communication session and replays some or all of it at a later time
  - Impersonation:
    - Attacker assumes the identity of one of the legitimate parties in a network
  - Man-in-the-Middle:
    - Attacker interposes himself between two parties and pretends to each to be the other
  - Interleaving attack:
    - Attacker injects spurious messages into a protocol run to disrupt or subvert it

Reply attack



transfer 100 euros into
the merchant's account



transfer 100 euros into
the merchant's account

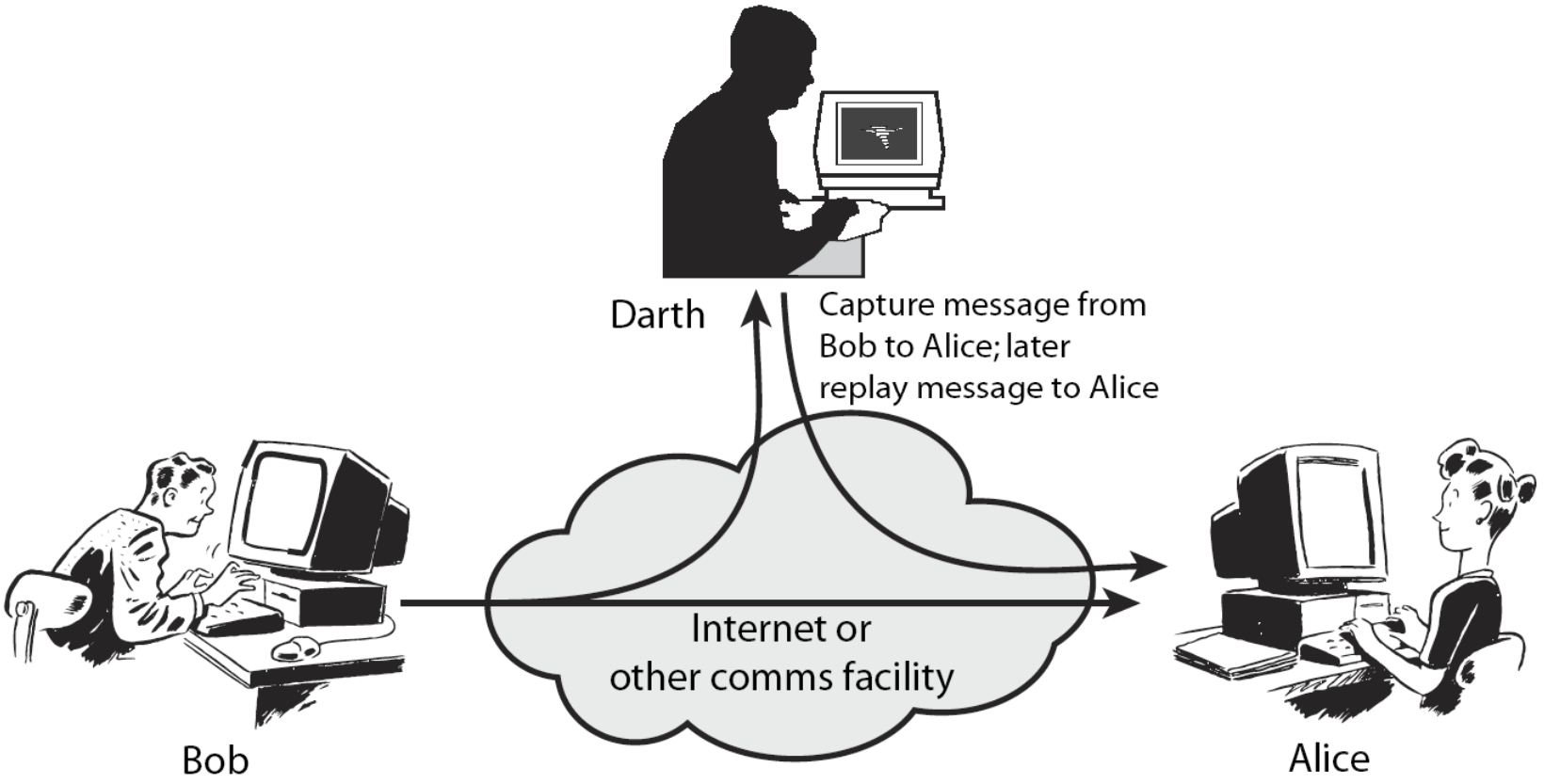
transfer 100 euros into
the account's merchant

⋮

transfer 100 euros into
the account's merchant

Source: Bruno Blanchet

Man-in-the-middle attack

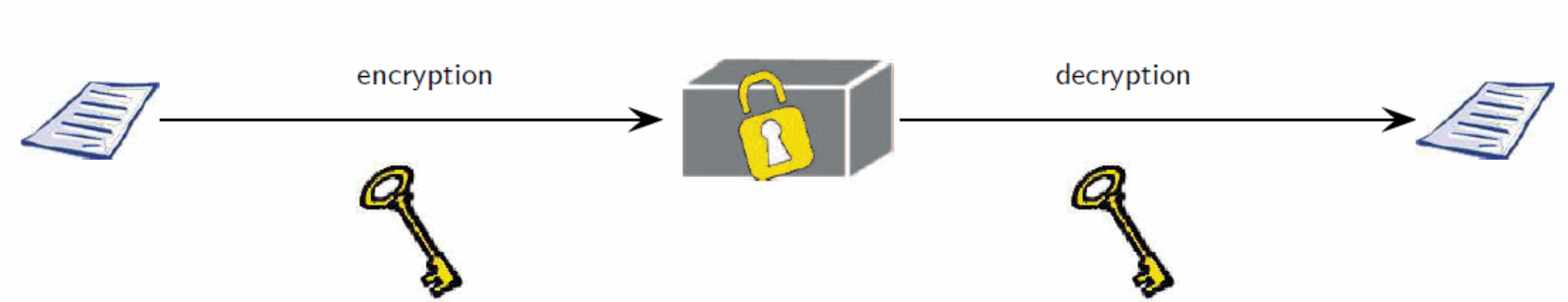


Cryptographic primitives

- Algorithms that are frequently used to build computer security systems
  - These routines include, but are not limited to, encryption and signature functions

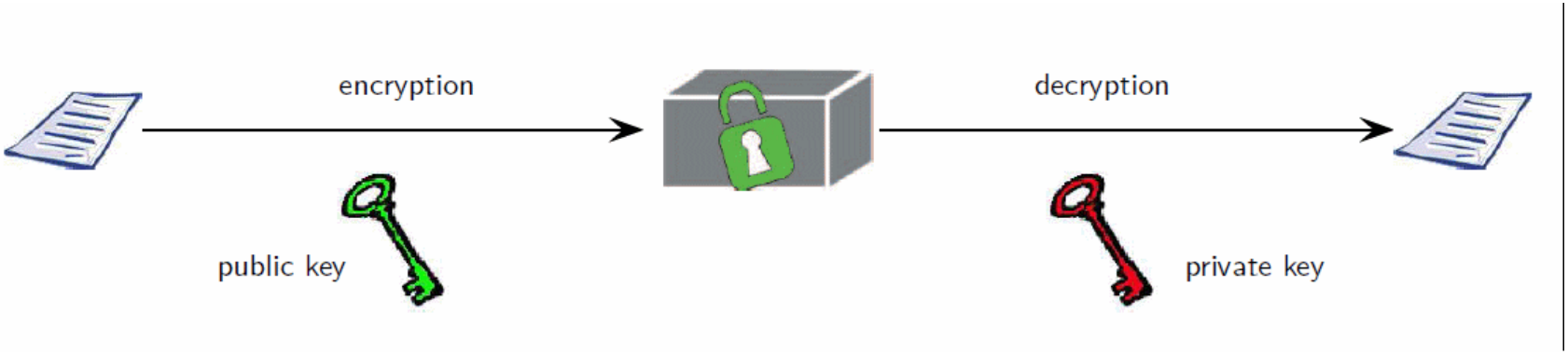
Symmetric encryption

- Key is a shared secret
- Same key to encrypt and decrypt



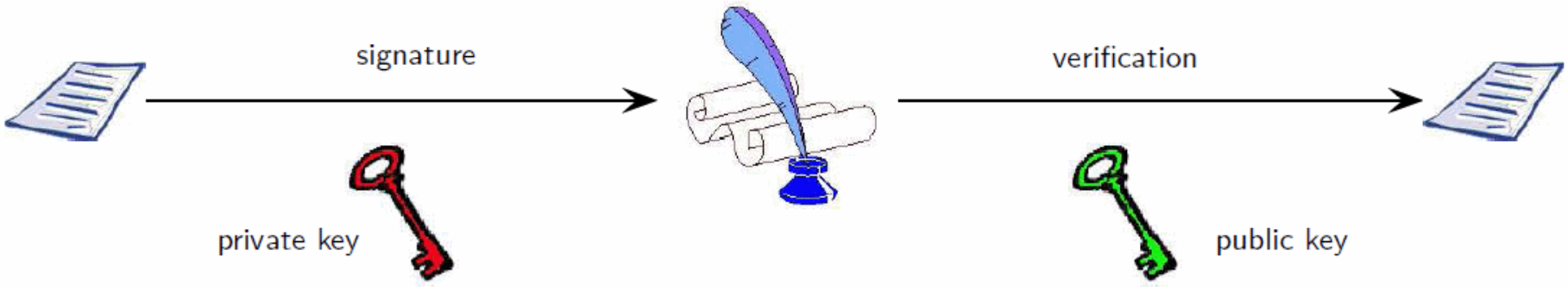
Asymmetric encryption

- Uses a mathematically related key pair
  - Public key to encrypt
  - Private key to decrypt
- Bob gives away the public key to all his friends so they can encrypt messages for him
- Are considered slow

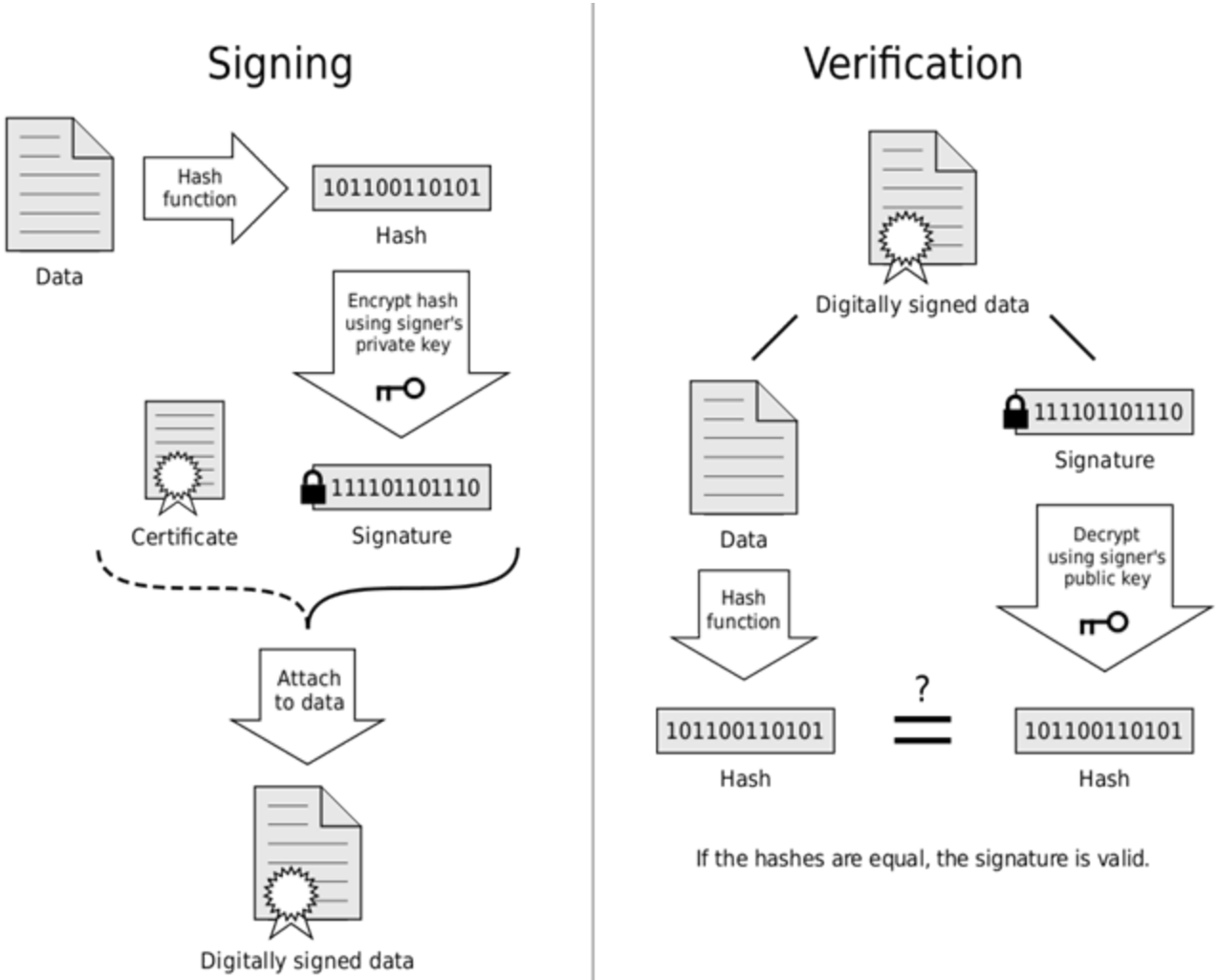


Signature

- Derived from the message content
  - May sign part of the message
- Offer
  - Guarantee the message has not been tamper with
  - Non-repudiation



Signature



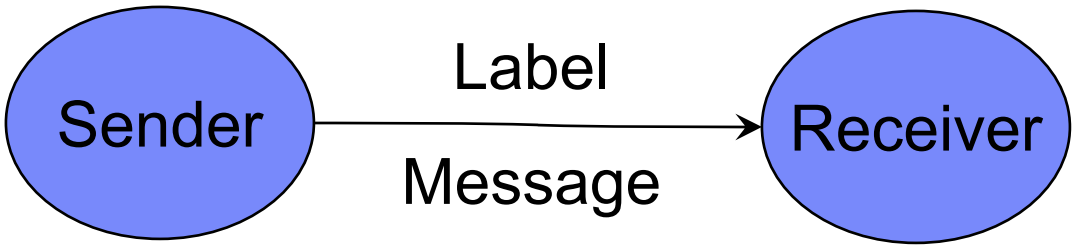
Source: http://en.wikipedia.org/wiki/File:Digital_Signature_diagram.svg

Protocol terminology

- Steps in the form
  - [label.] sender -> receiver : message
- Label is optional
- Message terminology
  - K = key (subscripted to indicate origin)
  - N = nonce (number used once)
  - T = timestamp
  - {M}k = message M encrypted with key k
    - In some books may be $E_k(M)$ or E(k,M)
  - , = comma is used to separate the pieces of the message (but may not be included in the message

Protocol graph

- Note that “[label.] sender -> receiver :” describes a state machine
- It is easier to understand a protocol by drawing the state machine



Wide-Mouth Frog protocol

- Alice (A) and Bob (B) share a secret key with Trent (T)
- Protocol is used for key distribution
- Protocol

1. $A \rightarrow T : A, \{T_A, B, K_{AB}\}K_{AT}$
2. $T \rightarrow B : \{T_T, A, K_{AB}\}K_{BT}$

Needham Schroeder Symmetric Key protocol

- Distribution (steps 1-3) of a shared symmetric key (Kab) by a trusted server and mutual authentication (steps 4-5). By Roger Needham and Michael Schroeder (1978)
- Alice (A) and Bob (B) share a secret key with Trent (T)
- Protocol
  - 1. A -> T : A,B,N_a
  - 2. T -> A : $\{N_a,B,K_{ab}, \{K_{ab},A\}K_{bt} \}K_{at}$
  - 3. A -> B : $\{K_{ab},A\}K_{bt}$
  - 4. B -> A : $\{N_b\}K_{ab}$
  - 5. A -> B : $\{N_b - 1\}K_{ab}$

Kerberos protocol

- Derive from Needham-Schroeder
- Alice (A) wants to use a resource (B), so she ask for a ticket to the server (S)
- Protocol
  - $A \rightarrow S : A, B$
  - $S \rightarrow A : \{T_S, L, K_{AB}, B, \{T_S, L, K_{AB}, A\}K_{BS}\} K_{AS}$
  - $A \rightarrow B : \{T_S, L, K_{AB}, A\}K_{BS} , \{A, T_A\} K_{AB}$
  - $B \rightarrow A : \{T_A+1\}K_{AB}$
- Introduce lifetime (L) and the concept of a token or ticket $\{T_S, L, K_{AB}, A\}K_{BS}$

The End