Cryptography
6CCS3CIS / 7CCSMCIS

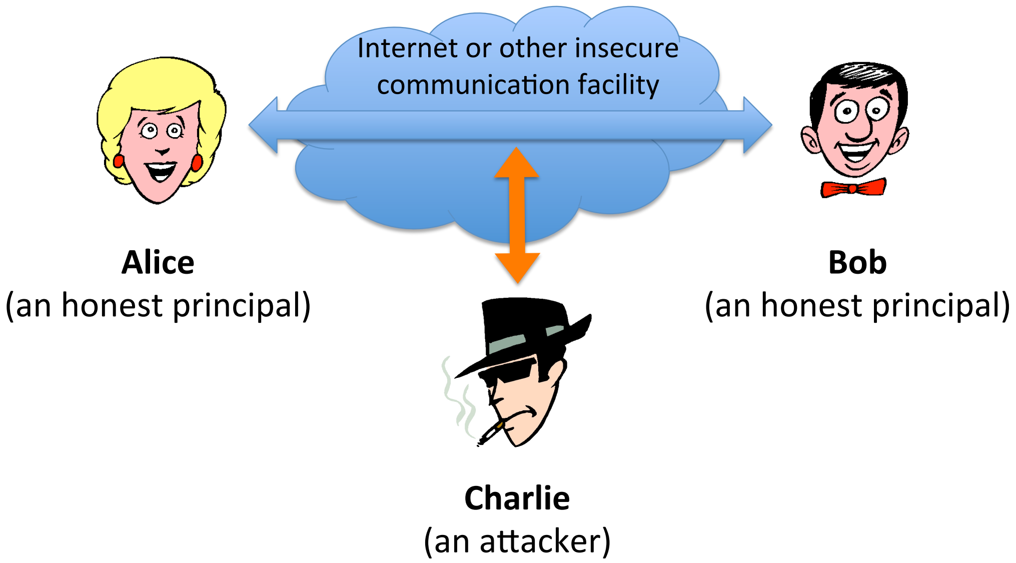
Prof. Luca Viganò

Department of Informatics
King’s College London, UK

First term 2020/21

Lecture 1.3: Security properties — Confidentiality

What’s it all about?



Internet or other insecure communication facility

Alice
(an honest principal)

Bob
(an honest principal)

Charlie
(an attacker)

How do we turn an insecure communication facility (like the Internet) into a secure one?

Where security means that one or more security properties (e.g., confidentiality, integrity, authentication, non-repudiation, anonymity, unobservability, timeliness, availability, etc.) are guaranteed.

Cryptography is an enabling technology.

Traditional security properties/goals

- Common security properties spell out the acronym CIA:

  Confidentiality (Secrecy): No improper disclosure of information.

  Integrity: No improper modification of information.

  Availability: No improper impairment of functionality/service.

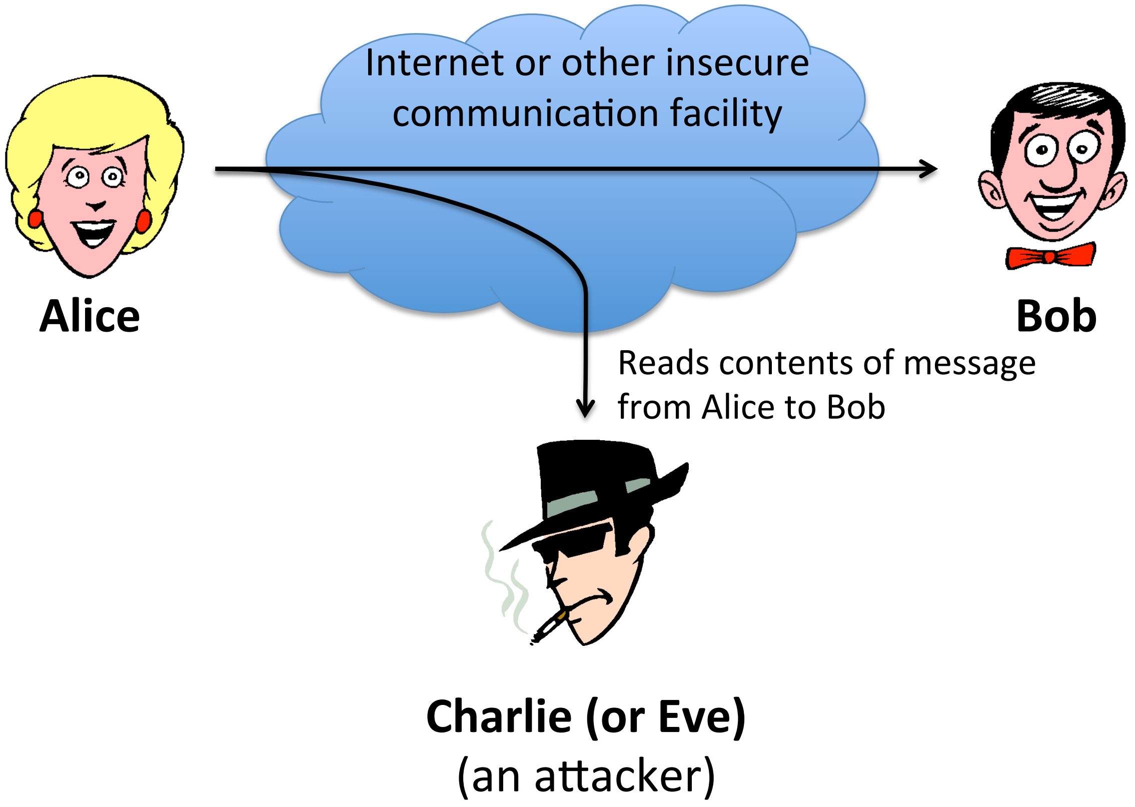
- Note that:
  - (Im)proper must be specified individually, for each system.
  - Alternatively, they can be formulated as:

    Confidentiality: No unauthorized access to information.
    Integrity: No unauthorized modification of information.
    Availability: No unauthorized impairment of functionality.

Security properties/goals: confidentiality (i.e., secrecy)

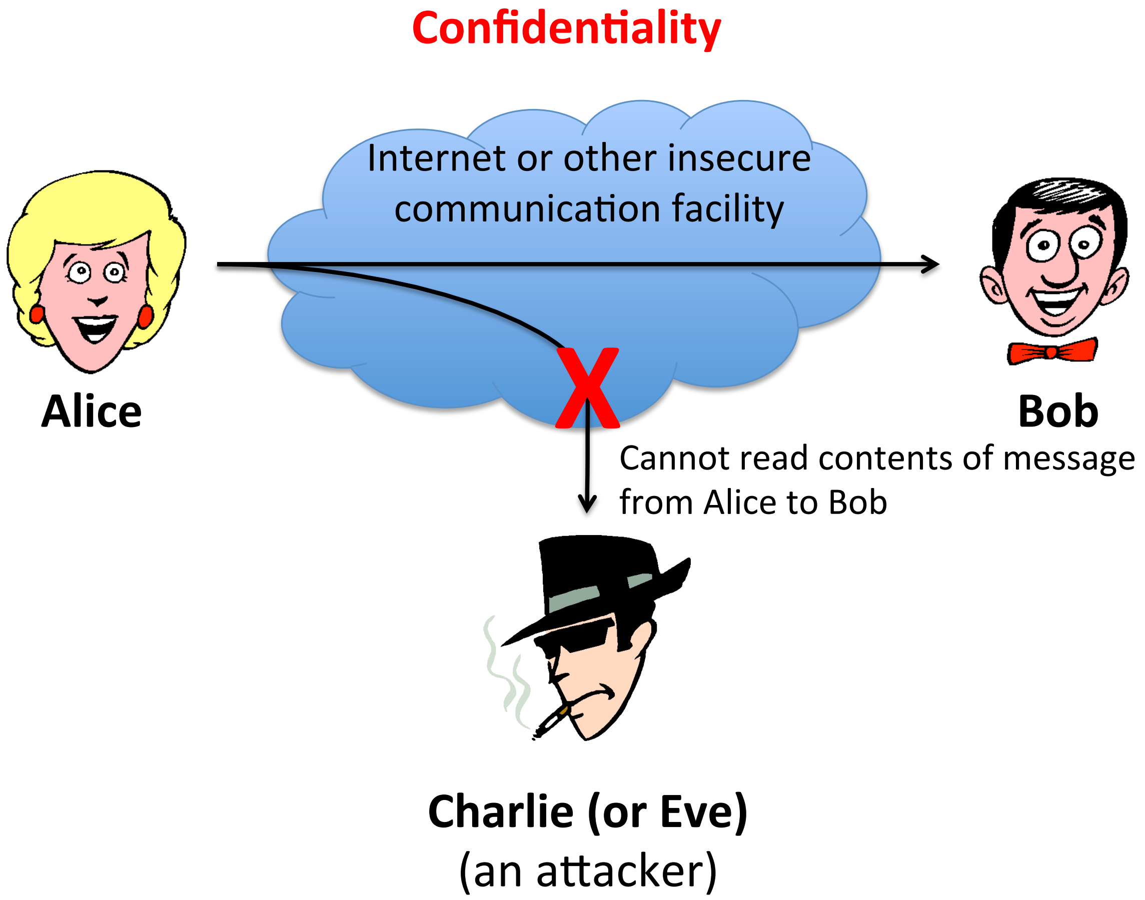
Confidentiality *information is not learned by unauthorized principals*

Attack against confidentiality (passive attack)


Internet or other insecure communication facility
Alice
Bob
Reads contents of message from Alice to Bob
Charlie (or Eve)
(an attacker)

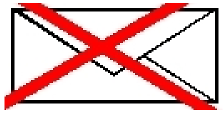
Security properties/goals: confidentiality (i.e., secrecy)

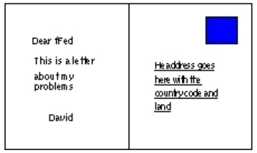
Confidentiality *information is not learned by unauthorized principals*

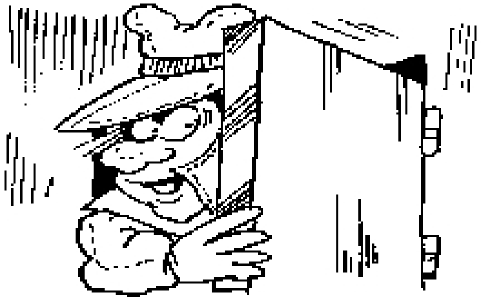

Confidentiality
Internet or other insecure communication facility
Alice
Bob
X
Cannot read contents of message from Alice to Bob
Charlie (or Eve)
(an attacker)

Confidentiality is guaranteed whenever Charlie, who is not authorised to read the message, is not able to read the message.

Confidentiality

Example Email is **not** a letter 

but rather a post card! 



Threat Everyone can read it along the way!

Mechanism Network security, encryption, and access control

Challenges Key and policy management.

Confidentiality, privacy and anonymity

Information is not learned by unauthorized principals

- Confidentiality is sometimes characterised as the unauthorized reading of data, when considering **access control** measures. But in general we are concerned with unauthorized learning of information, which is more subtle to contend with.
- Confidentiality presumes a notion of authorized party, or more generally, a **security policy** saying who or what can access our data. The security policy is used for access control.
- Sometimes: **privacy** pertains to confidentiality for individuals, whereas **secrecy** pertains to confidentiality for organizations, such as commercial companies or governments. Privacy is also sometimes used in the sense of **anonymity**, keeping one's identity private.
- Example violations: your medical records are obtained by a potential employer without your permission; "somebody" finds out which websites you are accessings.

More on privacy and anonymity

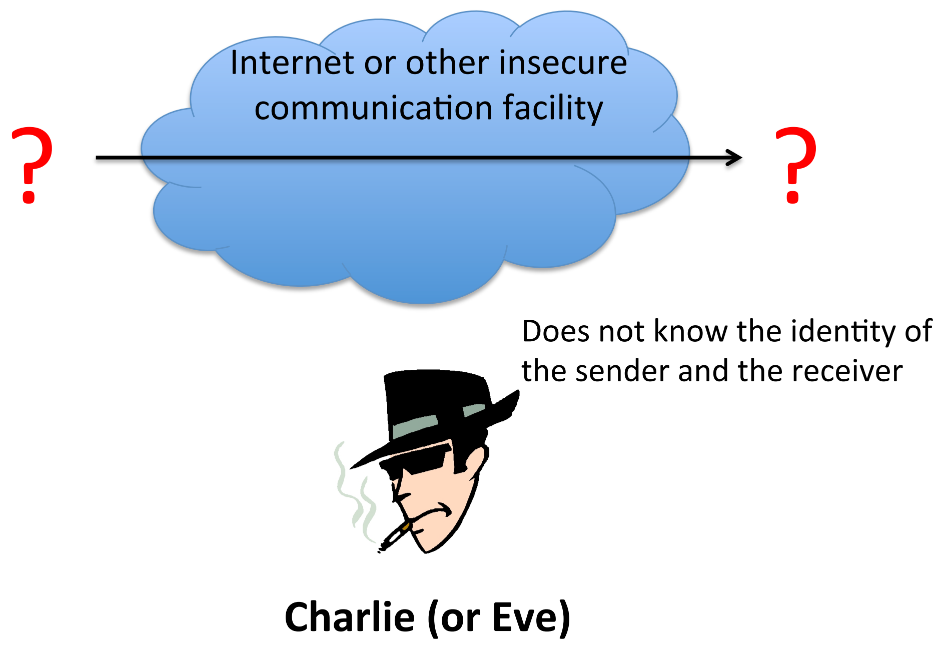
Privacy:

- *You choose what you let other people know*.
- Confidentiality of information that you don't want to share.

Anonymity:

- *A condition in which your true identity is not known*.
- Confidentiality of your identity.

Anonymity


Internet or other insecure communication facility
?
?
Does not know the identity of the sender and the receiver

Charlie (or Eve)

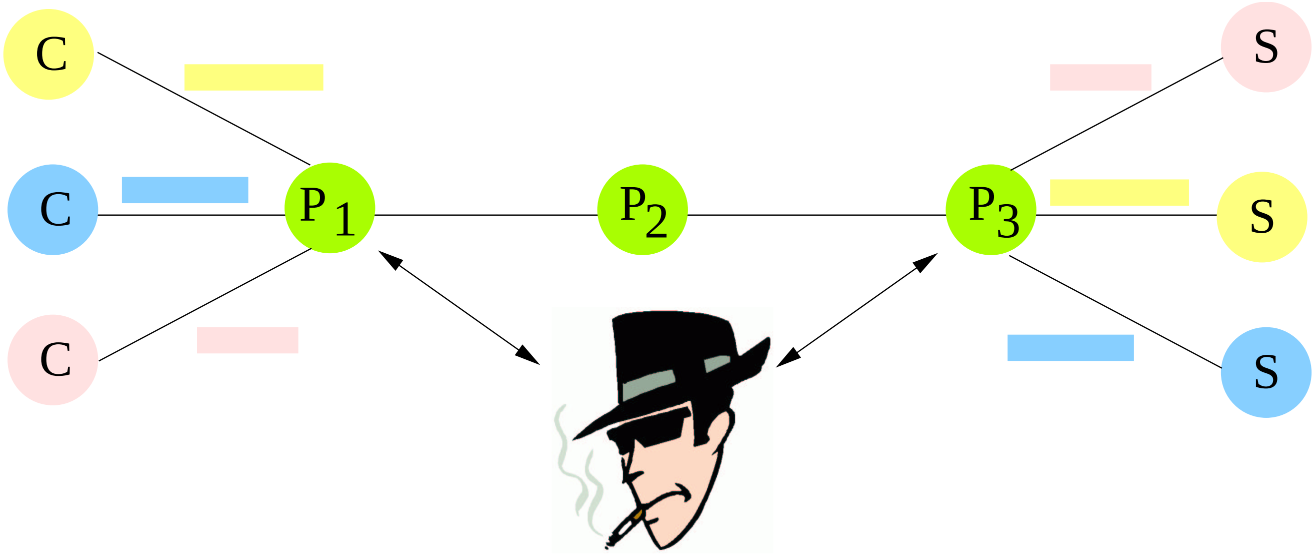
Privacy and anonymity on public networks

- **Internet is designed as a public network.**
    - Machines on your LAN may see your traffic, network routers see all traffic that passes through them.
    - Email is not a letter but rather a post card! (Everyone can read it along the way.)
- **Routing information is public.**
    - IP packet headers identify source and destination.
    - Even a passive observer can easily figure out *who is talking to whom*.
- **Encryption does not hide identities.**
    - Encryption hides payload, but not routing information.
    - Even IP-level encryption (tunnel-mode IPsec/ESP) reveals IP addresses of IPsec gateways.

Why is anonymity difficult?

In a public network:

- Packet headers identify recipients.
- Packet routes can be tracked (traffic analysis).



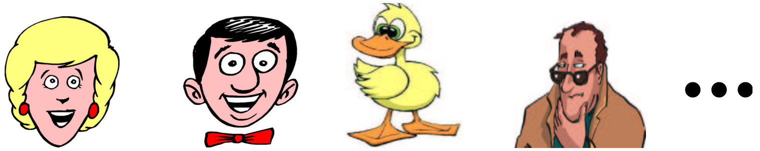
Someone observing P_1 and P_3 can usually break anonymity.

- Payload, even when encrypted, is visible.
- Short delay between messages entering P_1 and P_3.

Challenge is to design technologies to thwart such analysis.

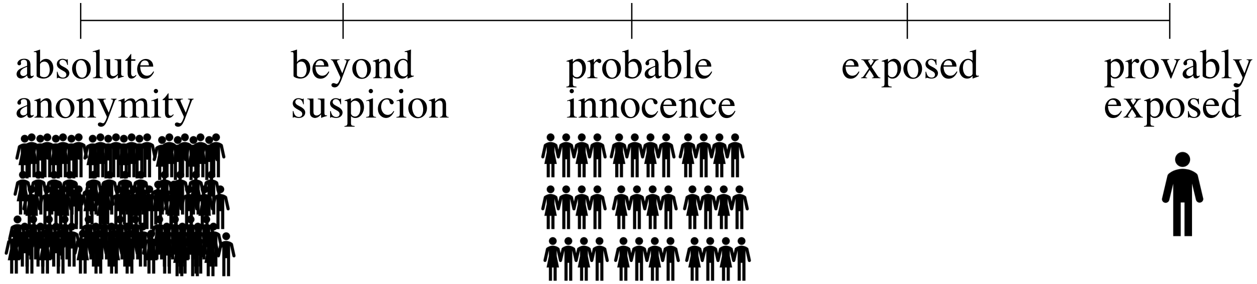
What is anonymity?

- Your actions can be observed (e.g., sending/receiving emails).



You are only anonymous within a group if your actions (sending, receiving, communication relationships) cannot be distinguished from the actions of anyone else in a group.

- This group is called the **anonymity set**. The larger, the better.



absolute anonymity

beyond suspicion

probable innocence

exposed

provably exposed

- You cannot be anonymous by yourself!
  - Big difference between anonymity and confidentiality.
- Anonymity is best when anonymizing service attracts many users.
  - All existing technologies have performance/reliability overheads.
  - Usability is central to success.

Some possible applications of privacy and anonymity

- **Privacy**:
  - Hide online transactions, Web browsing, etc. from intrusive governments, marketers and archivists.
- **Untraceable electronic mail**:
  - Corporate whistle-blowers.
  - Political dissidents.
  - Socially sensitive communications (online AA meeting).
  - Confidential business negotiations.
- **Law enforcement and intelligence**:
  - Sting operations and honeypots.
  - Secret communications on a public network.
- **Blockchain, Cryptocurrencies, Digital cash**:
  - Electronic currency with properties of paper money (online purchases unlinkable to buyer's identity).
- **Anonymous electronic voting**.
- **Censorship-resistant publishing**.
- **Crypto-anarchy**.

Attacks on anonymity

- **Passive traffic analysis**:
  - Infer from network traffic who is talking to whom.
  - To hide your traffic, must carry other people's traffic!
- **Active traffic analysis**:
  - Inject packets or put a timing signature on packet flow.
- **Compromise of network nodes (routers)**:
  - It is not obvious which nodes have been compromised
    - Attacker may be passively logging traffic.
  - Better not to trust any individual node
    - Assume that some *fraction* of nodes is good, don't know which.

Anonymity, unlinkability, unobservability

- Summarizing: **Anonymity** is the state of being not identifiable within a set of subjects.
  - Hide your activities among others' similar activities.
- **Unlinkability** of action and identity.
  - For example, sender and his email are no more related after observing communication than they were before.
- **Unobservability** (hard to achieve).
  - Observer cannot even tell whether a certain action took place or not.