CS396: Security, Privacy & Society

Fall 2022

Lecture 5: Cryptographic System I

Instructor: Abrar Alrumayh

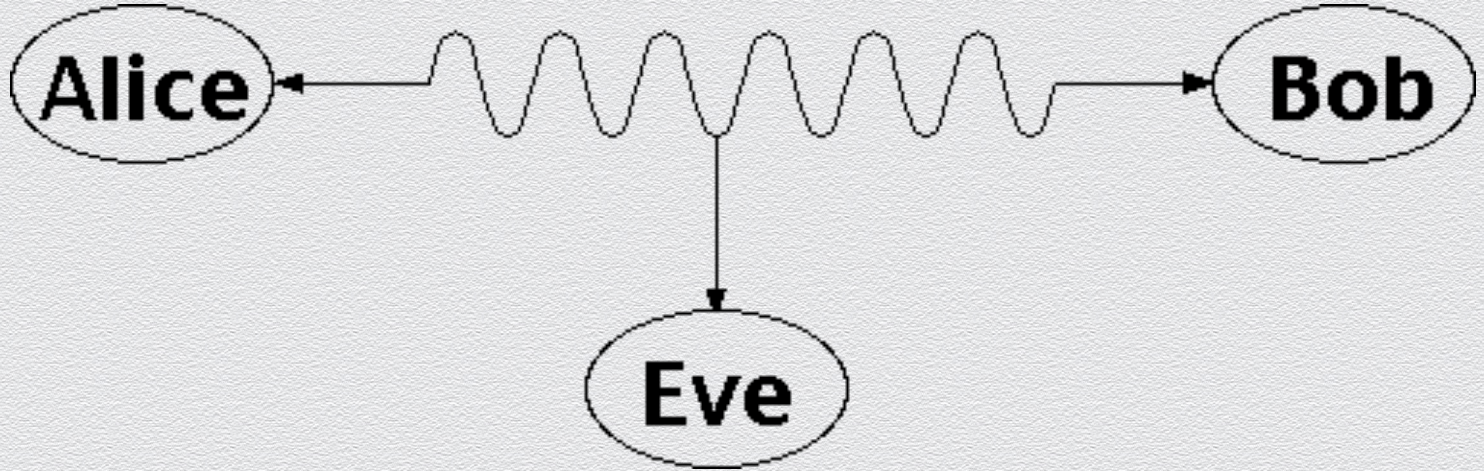
September 14, 2022

Outline

- Basic concepts and terms
- Cryptographic System I
  - Symmetric-key Encryption

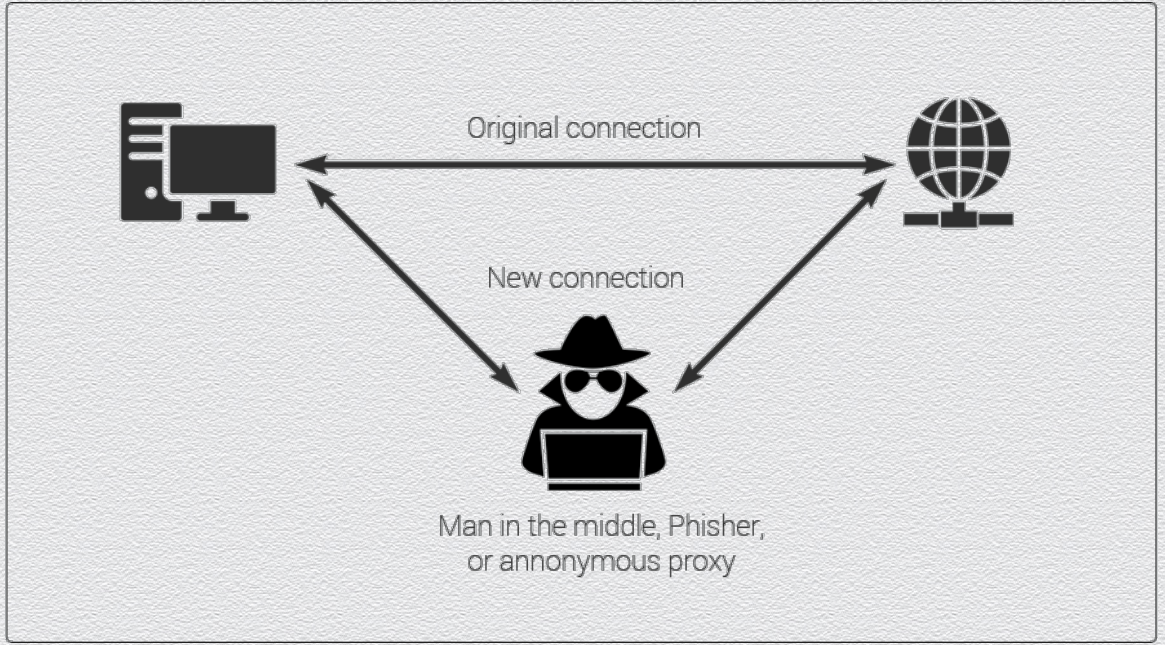
Example of threat

- **Eavesdropping:** the interception of information intended for someone else during its transmission over a communication channel



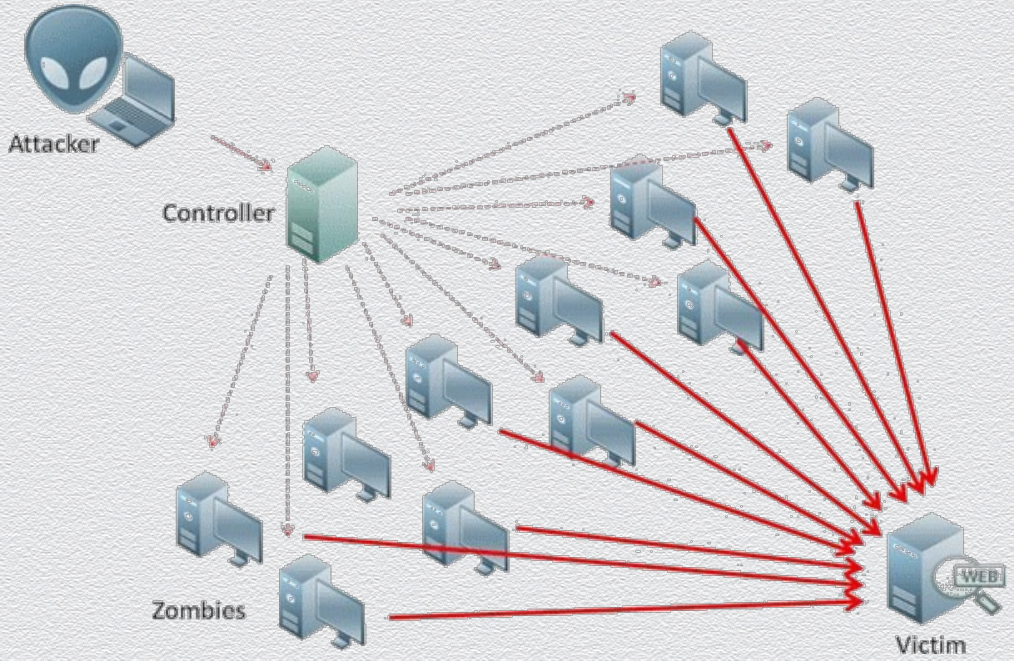
Example of threat

- **Alteration:** unauthorized modification of information
  - **Example:** the man-in-the-middle attack, where a network stream is intercepted, modified, and retransmitted



Example of threat

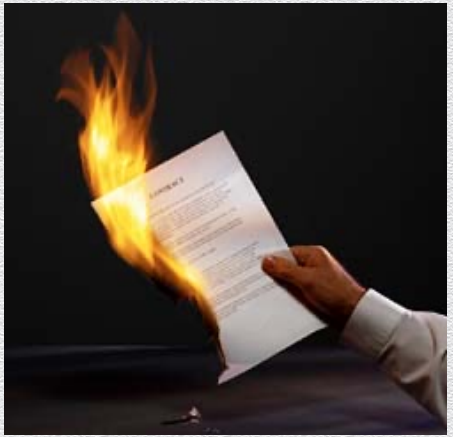
- **Denial-of-service:** the interruption or degradation of a data service or information access
  - **Example:** email **spam,** to the degree that it is meant to simply fill up a mail queue and slow down an email server



Examples of threats

- **Masquerading**: the fabrication of information that is claimed to be from someone who is not actually the author
  - e.g., IP spoofing attack: maliciously altering the source IP address of a message

- **Repudiation:** the denial of a commitment or data receipt
  - this involves an attempt to back out of a contract/protocol that, e.g., requires the different parties to provide receipts acknowledging that data has been received



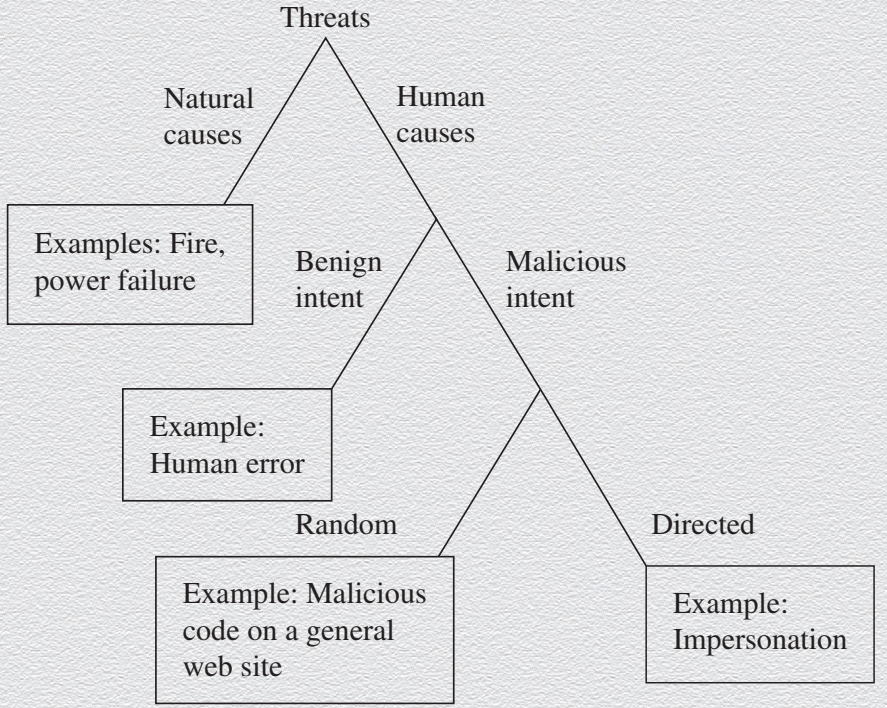
Example of vulnerability

- **Software bugs:** Code is not doing what is supposed to be doing
  - **Example:** Some application code is mistakenly using an algorithm for encryption that has been broken
  - **Example:** There is no checking of array bounds

An hard-to-win game: Varied threats

Threats

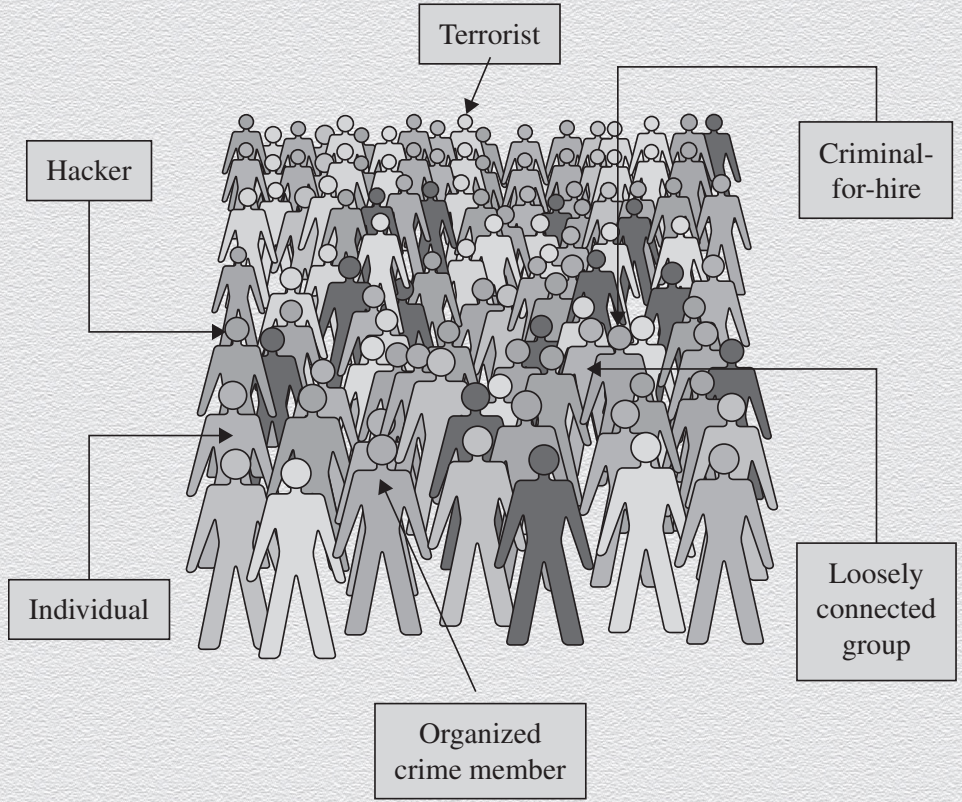
- from natural to human
- from benign to malicious
- from random to targeted (APTs)



A hard-to-win game: Unknown enemy

Attackers

- beyond isolated “crazy” hackers
- organized groups/crime
  - may use computer crime (e.g., stealing CC#s) in order to finance other crimes
- terrorists
  - computers/assets as target, method, enabler, or enhancer

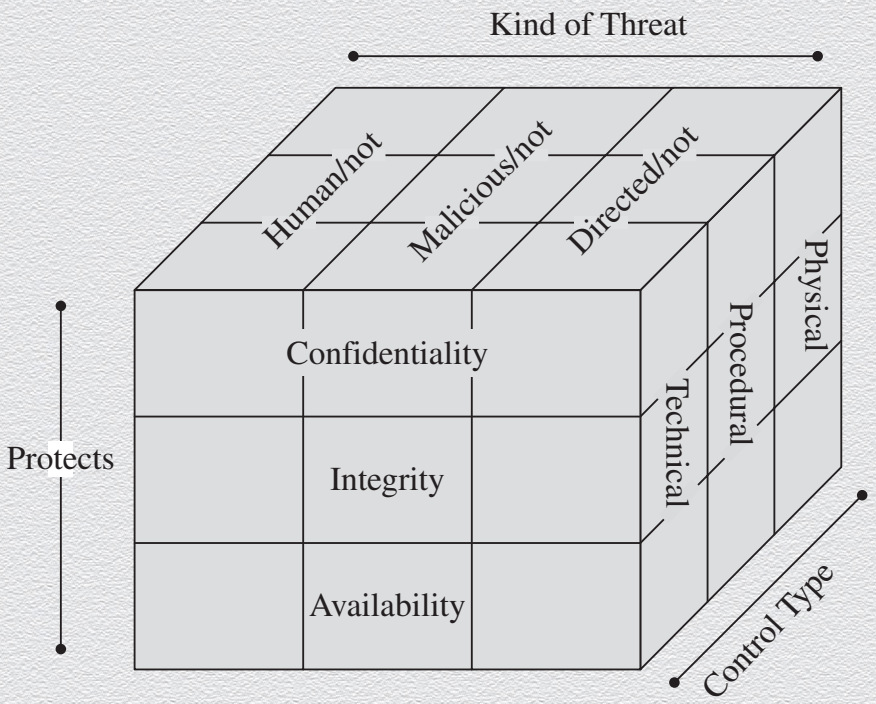


A hard-to-win game: Choose your battle

Risk management

- choose priorities
  - which threats to control
    - estimate possible harm & impact
  - what / how many resources to devote
    - estimate solution cost & protection level
- consider trade-offs balancing cost Vs. benefit
- compute the **residual risk**
  - decide on transfering risk or doing nothing

Never a “one-shot” game



A hard-to-win game: Best-effort approach

Deciding on controls relies on incomplete information

- likelihood of attack and impact of possible harm is impossible to measure perfectly
- full set of vulnerabilities is often unknown
  - weak authentication, lack of access control, errors in programs, etc.
- system's attack surface is often too wide
  - physical hazards, malicious attacks, stealthy theft by insiders, benign mistakes, impersonations, etc.

A useful strategy: The "method – opportunity – motive" view of an attack

- **deny any of them and the attack will (likely) fail**

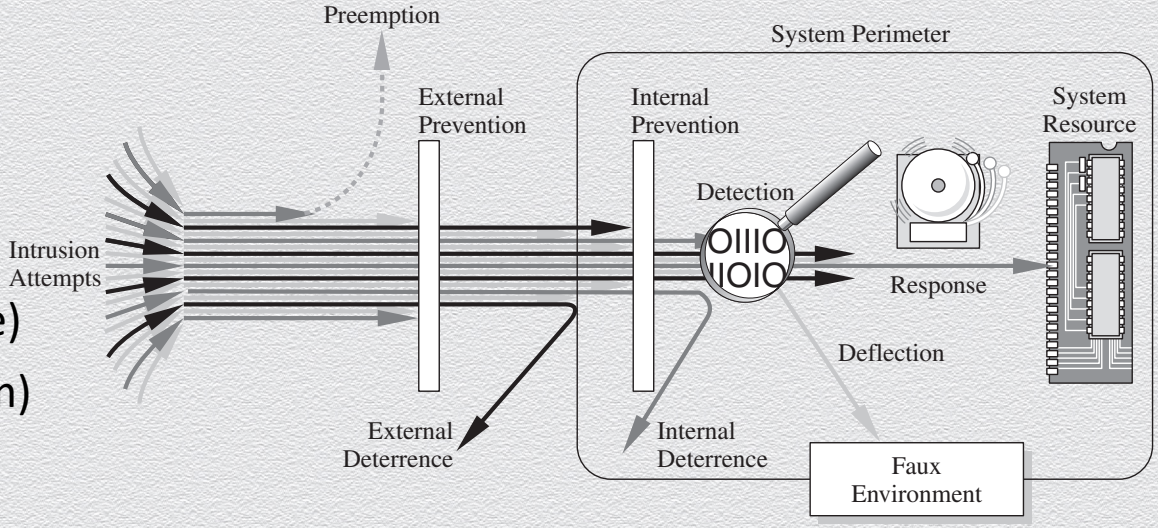
A hard-to-win game: Best-effort approach (continued)

Controls offer a wide range of protection level / efficacy

- they counter or neutralize threats or remove vulnerabilities in different ways

Types of controls

- prevent (attack is blocked)
- deter (attack becomes harder)
- deflect (change target of attack)
- mitigate (make impact less severe)
- contain (stop propagation of harm)
- detect (real time/after the fact)
- recover (from its effects)



Hard to balance cost/effectiveness of controls with likelihood/severity of threats

Example of control: HTTPS protocol

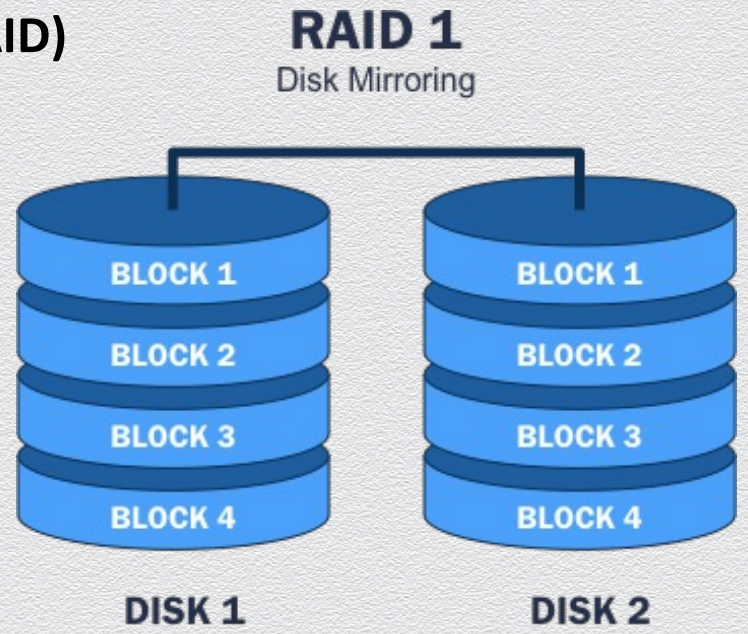
Hypertext Transfer Protocol Secure (HTTPS)

- Confidentiality
- Integrity
- Availability
- Authenticity
- Anonymity

Example of control: RAID technology

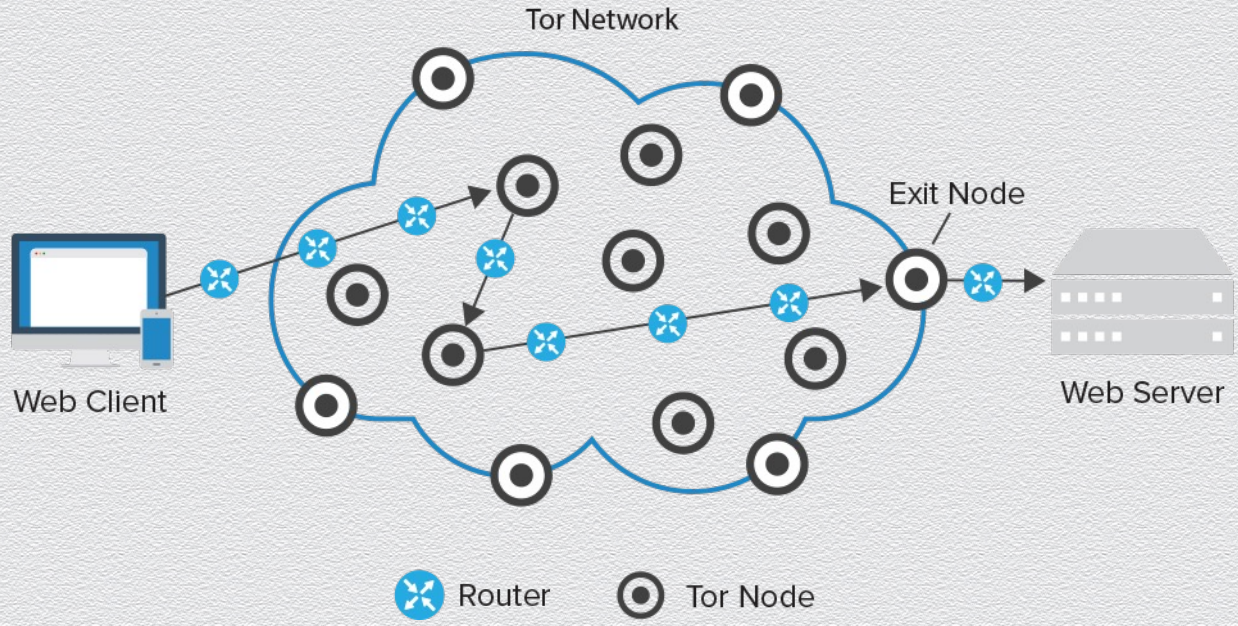
Redundant Array of Independent Disks (RAID)

- Confidentiality
- Integrity
- Availability
- Authenticity
- Anonymity



Example of controls: TOR protocol

- Confidentiality
- Integrity
- Availability
- Authenticity
- Anonymity



As we will see: Exciting times to study (or work in) IT Security!

Relevance to practice & real-world importance

- plethora of real-world problems & real needs for security solutions
- combination of different research areas within CS and across other fields
- multi-dimensional topic of study
  - protocol design, system building, user experience, social/economic aspects
- wide range of perspectives
  - practical / systems – foundations / theory, attacker's Vs. defender's view

Symmetric-key encryption

Recall: Confidentiality

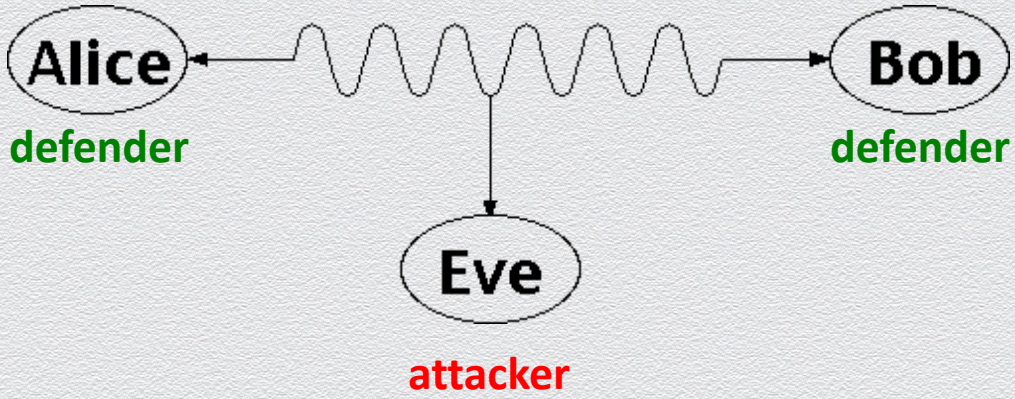
Fundamental security property

- **an asset is viewed only by authorized parties**
- "C" in the CIA triad

> *"computer security seeks to prevent **unauthorized viewing (confidentiality)** or modification (integrity) of **data** while preserving access (availability)"*

Eavesdropping

- main threat against confidentiality of **in-transit** data



Problem setting: Secret communication

Two parties wish to communicate over a channel

- Alice (sender/source) wants to send a message m to Bob (recipient/destination)

Underlying channel is unprotected

- Eve (attacker/adversary) can eavesdrop any sent messages
- e.g., packet sniffing over networked or wireless communications

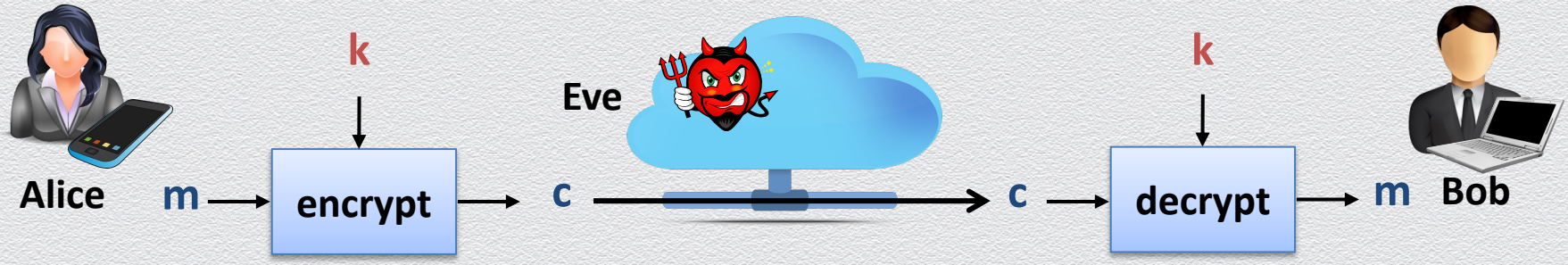
Alice m

m Bob

Solution concept: Symmetric-key encryption

Main idea

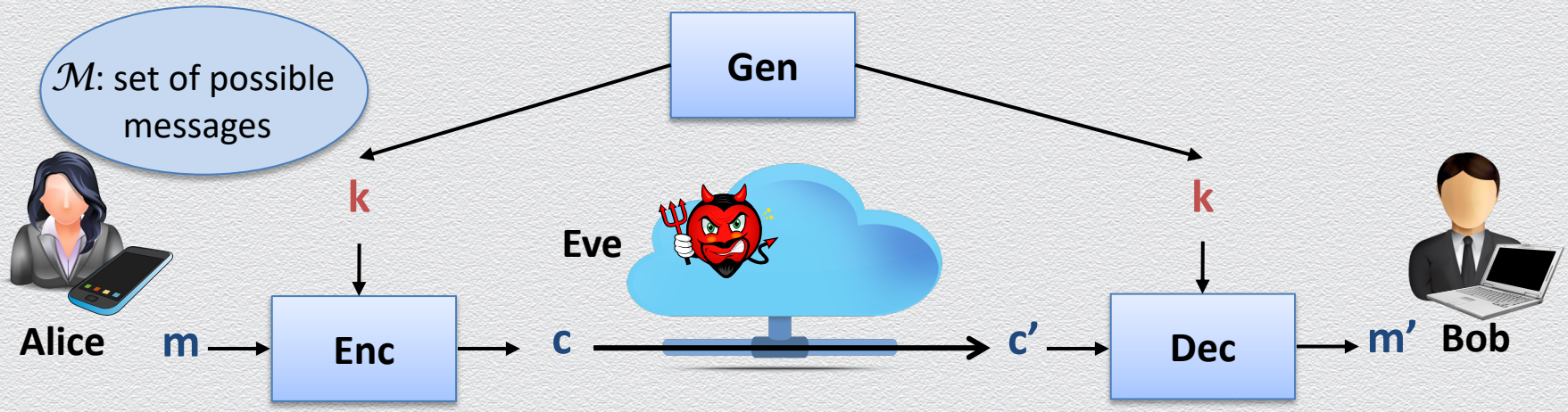
- secretly transform message so that it is **unintelligible** while in transit
  - Alice **encrypts** her message m to **ciphertext c**, which is sent instead of **plaintext m**
  - Bob **decrypts** received message c to original message m
  - Eve can intercept c but "**cannot learn**" m from c
  - Alice and Bob share a **secret key k** that is used for both message transformations



Security tool: Symmetric-key encryption scheme

Abstract cryptographic primitive, **a.k.a. cipher**, defined by

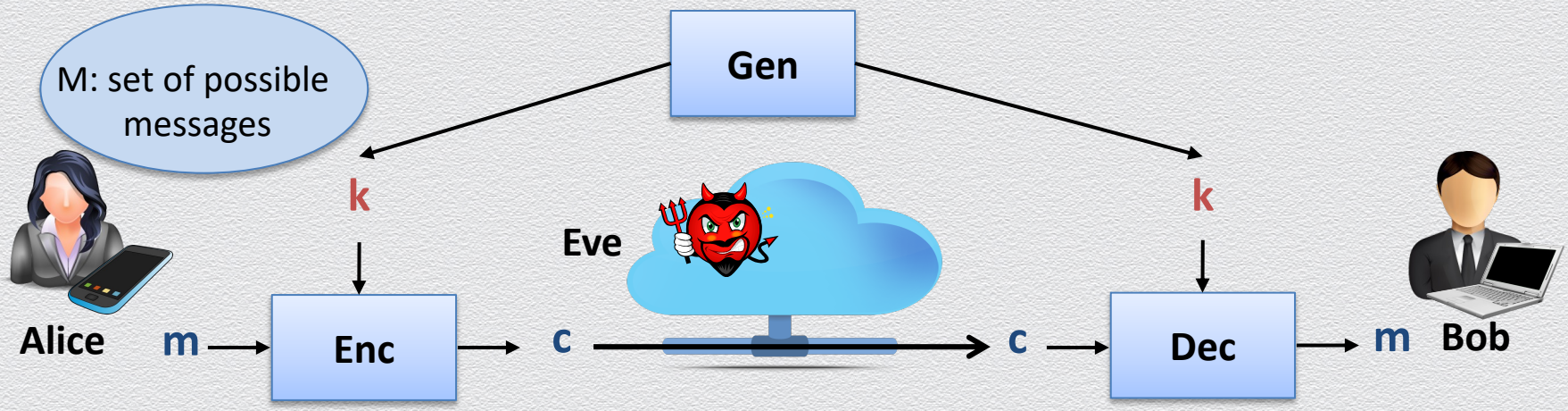
- a **message space $\mathcal{M}$**; and
- a triplet of algorithms **(Gen, Enc, Dec)**
  - Gen, Enc are probabilistic algorithms, whereas Dec is deterministic
  - Gen outputs a uniformly random key k (from some key space $\mathcal{K}$)



Desired properties for symmetric-key encryption scheme

By design, any symmetric-key encryption scheme should satisfy the following

- **efficiency**: key generation & message transformations "are fast"
- **correctness**: for all m and k, it holds that Dec(Enc(m, k) , k) = m
- **security**: one "cannot learn" plaintext m from ciphertext c



Kerckhoff's principle

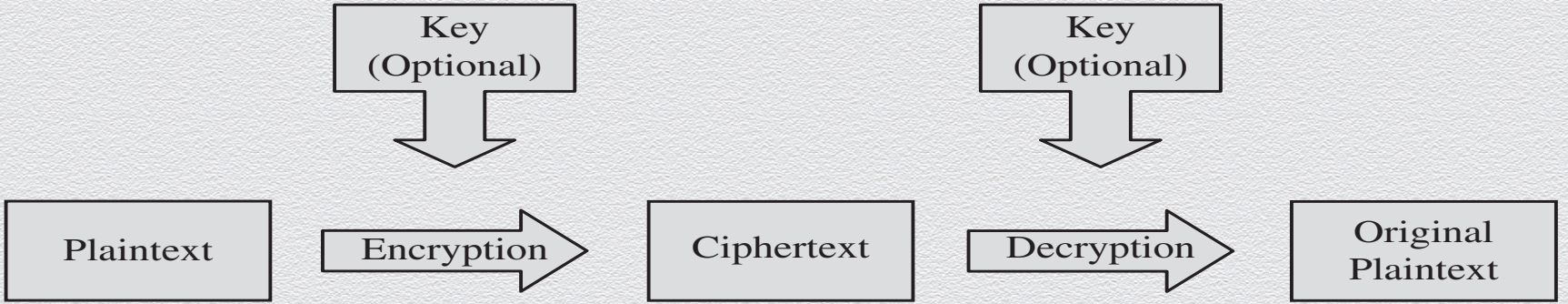
"The cipher method must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience."

Reasoning

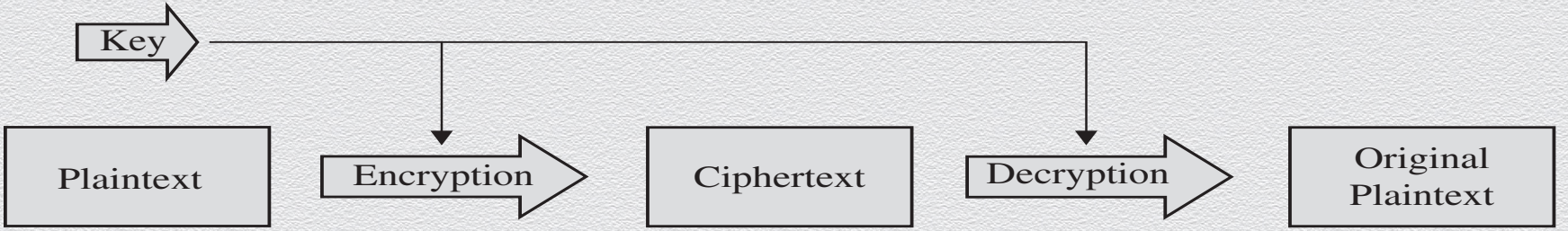
- due to security & correctness, Alice & Bob must share some secret info
- if no shared key captures this secret info, it must be captured by Enc, Dec
- but keeping Enc, Dec secret is problematic
  - harder to keep secret an algorithm than a short key (e.g., after user revocation)
  - harder to change an algorithm than a short key (e.g., after secret info is exposed)
  - riskier to rely on custom/ad-hoc schemes than publicly scrutinized/standardized ones

Symmetric-key encryption

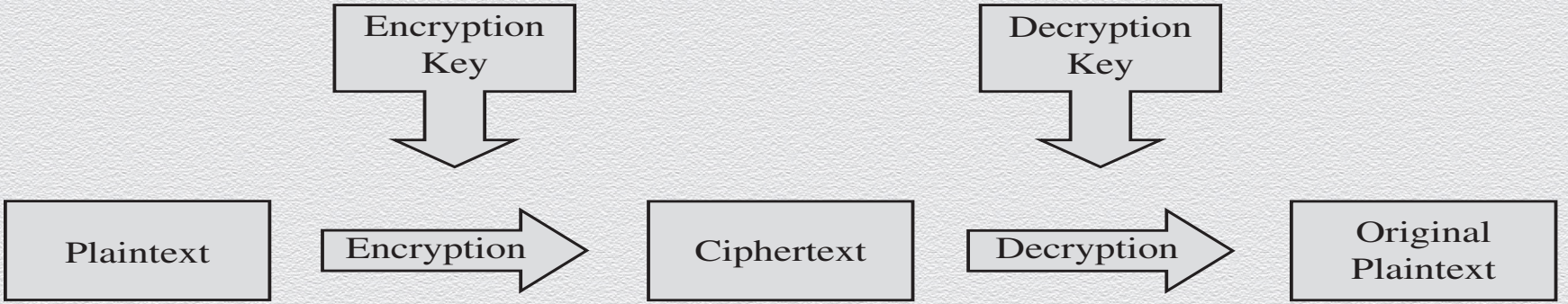
- Also referred to as simply “symmetric encryption”



Symmetric Vs. Asymmetric encryption



(a) Symmetric Cryptosystem



(b) Asymmetric Cryptosystem

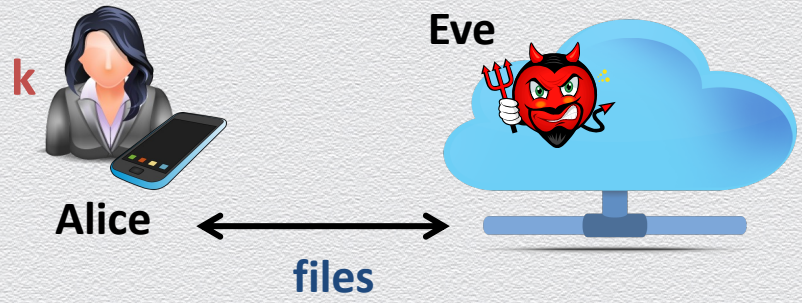
Main application areas

Secure communication

- **encrypt messages** sent among parties
- assumption
  - Alice and Bob **securely generate, distribute & store shared key k**
  - attacker does not learn key k

Secure storage

- **encrypt files** outsourced to the cloud
- assumption
  - Alice **securely generates & stores key k**
  - attacker does not learn key k



Brute-force attack

Generic attack

- given a captured ciphertext c and known key space $\mathcal{K}$, Dec
- strategy is an **exhaustive search**
  - for all possible keys k in $\mathcal{K}$
    - determine if Dec (c,k) is a likely plaintext m
- **requires some knowledge on the message space $\mathcal{M}$**
  - i.e., structure of the plaintext (e.g., PDF file or email message)

Countermeasure

- key should be a **random** value from a **sufficiently large** key space $\mathcal{K}$ to make exhaustive search attacks **infeasible**