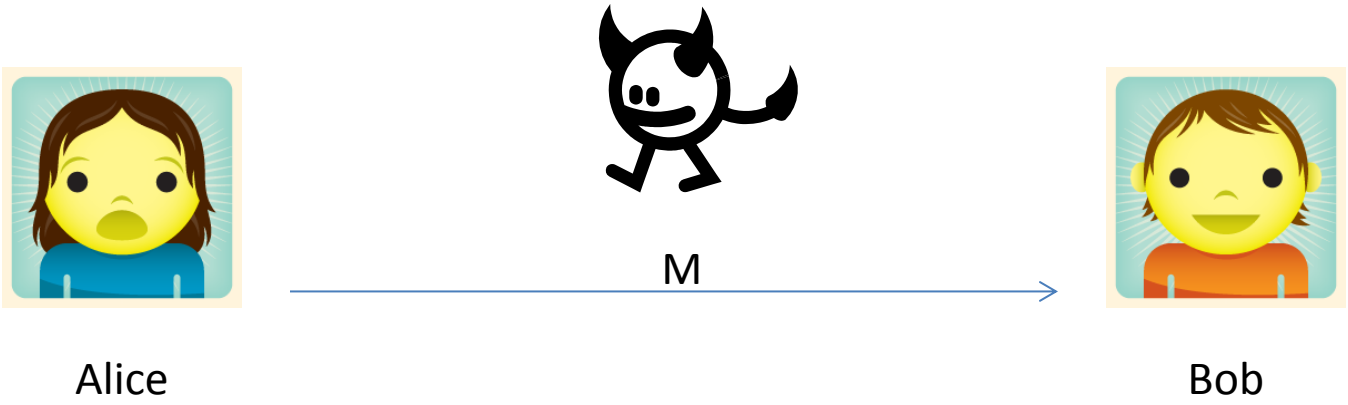
Goals of Modern Cryptography

- Providing information security:
  - Data Privacy
  - Data Integrity and Authenticity

  in various computational settings.

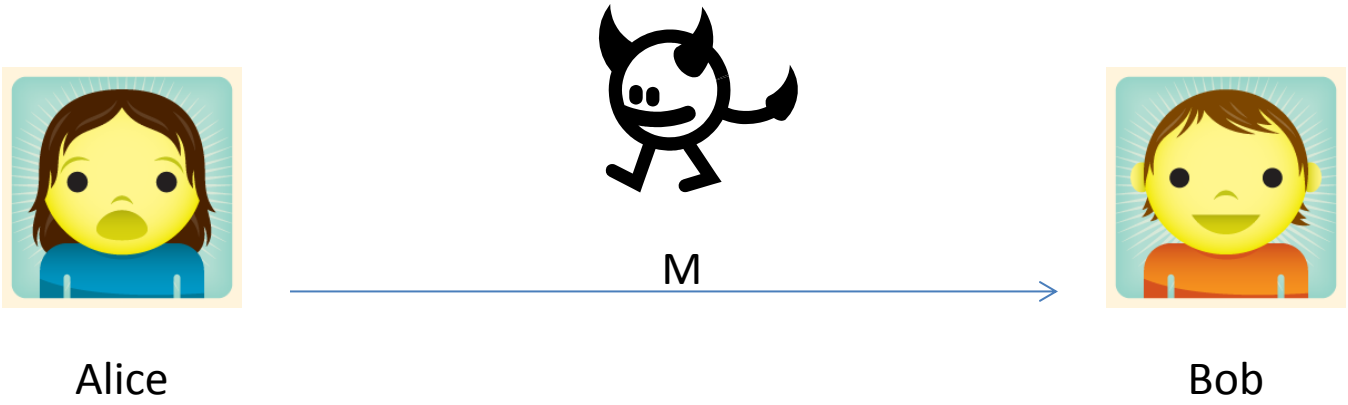
Data Privacy



The goal is to ensure that the adversary does not see or obtain the data (message) M.

- Example: M could be a credit card number being sent by shopper Alice to server Bob and we want to ensure attackers don't learn it.

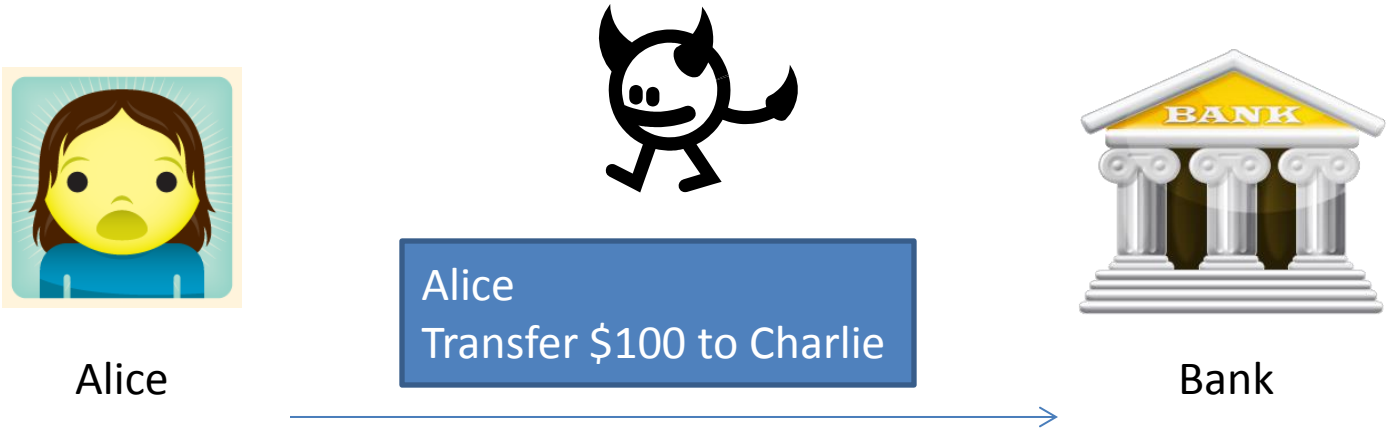
Data Integrity and Authenticity



The goal is to ensure that

- M really originates with Alice and not someone else.
- M has not been modified in transit.

Data Integrity and Authenticity



Adversary Eve might

- Modify “Charlie” to “Eve”
- Modify “$100” to “$1000”

Integrity prevents such attacks.

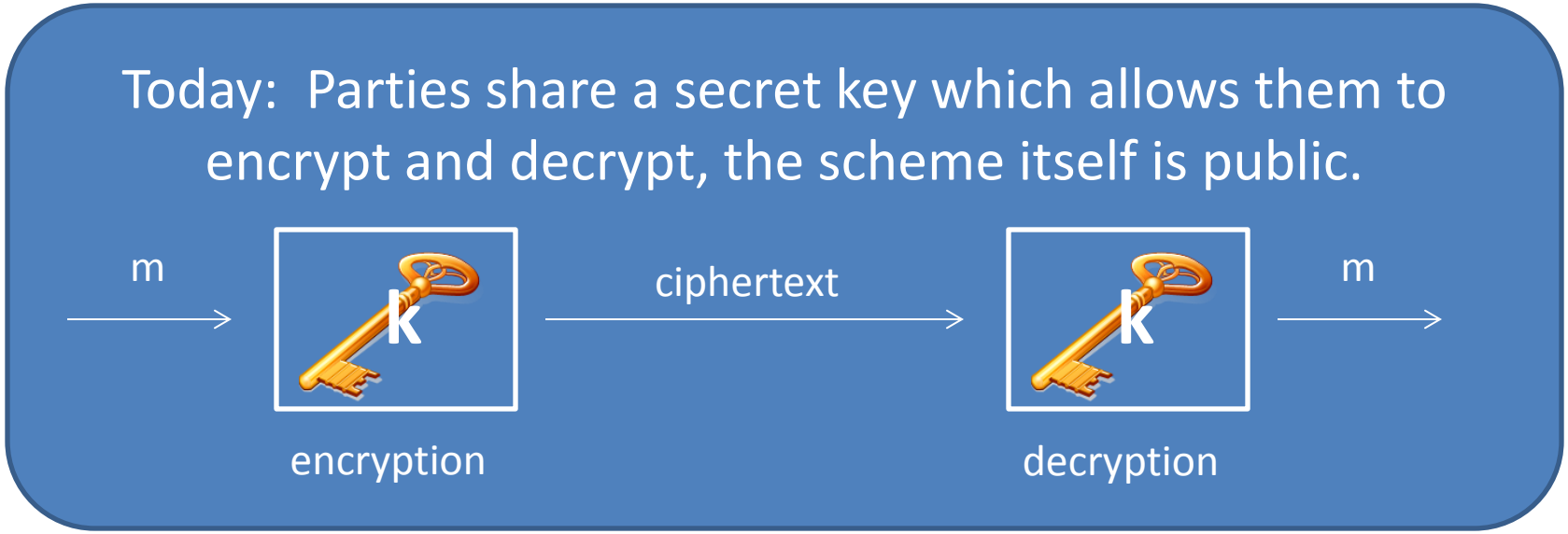
Symmetric Key Encryption (Historically called “ciphers”)

Kerckhoffs' Principle (1800s)

"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."

Kerckhoffs' Principle (1800s)

"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."



Advantages of open crypto design:

1. More suitable for large-scale usage.
   - All pairs of communicating parties can use the same scheme with different key.
2. Published designs undergo public scrutiny and are therefore likely to be stronger.
3. Public design enables the establishment of standards.

Coming up with the right definition

First Attempt:

"An encryption scheme is secure if no adversary can find the secret key when given a ciphertext"

Coming up with the right definition

First Attempt:

"An encryption scheme is secure if no adversary can find the secret key when given a ciphertext"

Problem: The aim of encryption is to protect the message, not the secret key.

Ex: Consider an encryption scheme that ignores the secret key and outputs the message.

Coming up with the right definition

Second Attempt:

"An encryption scheme is secure if no adversary can find the plaintext that corresponds to the ciphertext"

Coming up with the right definition

Second Attempt:

"An encryption scheme is secure if no adversary can find the plaintext that corresponds to the ciphertext"

Problem: An encryption scheme that reveals 90% of the plaintext would still be considered secure as long as it is hard to find the remaining 10%.

Coming up with the right definition

Third Attempt:

"An encryption scheme is secure if no adversary learns meaningful information about the plaintext after seeing the ciphertext"

Coming up with the right definition

Third Attempt:

"An encryption scheme is secure if no adversary learns meaningful information about the plaintext after seeing the ciphertext"

How do you formalize learns meaningful information?

Coming Up With The Right Definition

How do you formalize learns meaningful information?

Two ways:

- An information-theoretic approach of Shannon
- A computational approach (the approach of modern cryptography)

Formally Defining a Symmetric Key Encryption Scheme

Syntax

- An encryption scheme is defined by three algorithms
  - Gen, Enc, Dec
- Specification of message space $\boldsymbol{M}$ with $|\boldsymbol{M}| > 1$.
- Key-generation algorithm Gen:
  - Probabilistic algorithm
  - Outputs a key k according to some distribution.
  - Keyspace $\boldsymbol{K}$ is the set of all possible keys
- Encryption algorithm Enc:
  - Takes as input key $k \in \boldsymbol{K}$, message $m \in \boldsymbol{M}$
  - Encryption algorithm may be probabilistic
  - Outputs ciphertext $c \leftarrow Enc_k(m)$
  - Ciphertext space $\boldsymbol{C}$ is the set of all possible ciphertexts
- Decryption algorithm Dec:
  - Takes as input key $k \in \boldsymbol{K}$, ciphertext $c \in \boldsymbol{C}$
  - Decryption is deterministic
  - Outputs message $m := Dec\_k(c)$

Definition of Perfect Secrecy

- An encryption scheme (Gen, Enc, Dec) over a message space $\boldsymbol{M}$ is perfectly secret if for every probability distribution over $\boldsymbol{M}$, every message $m \in \boldsymbol{M}$, and every ciphertext $c \in \boldsymbol{C}$ for which $\Pr[C = c] > 0$:

$$\Pr[M = m \,|C = c] = \Pr[M = m]\,.$$

The One-Time Pad (Vernam's Cipher)

- In 1917, Vernam patented a cipher now called the one-time pad that obtains perfect secrecy.
- There was no proof of this fact at the time.
- 25 years later, Shannon introduced the notion of perfect secrecy and demonstrated that the one-time pad achieves this level of security.

The One-Time Pad Scheme

1. Fix an integer $\ell > 0$. Then the message space M, key space K, and ciphertext space C are all equal to $\{0,1\}^{\ell}$.
2. The key-generation algorithm Gen works by choosing a string from $K = \{0,1\}^{\ell}$ according to the uniform distribution.
3. Encryption Enc works as follows: given a key $k \in \{0,1\}^{\ell}$, and a message $m \in \{0,1\}^{\ell}$,output $c := k \oplus m$.
4. Decryption Dec works as follows: given a key $k \in \{0,1\}^{\ell}$, and a ciphertext $c \in \{0,1\}^{\ell}$, output $m := k \oplus c$.

Security of OTP

Theorem: The one-time pad encryption scheme is perfectly secure.