Foundations of Applied Cryptography

Adam O'Neill

Based on http://cseweb.ucsd.edu/~mihir/cse207/

Course Logistics

Instructor: Adam O’Neill,
https://groups.cs.umass.edu/oneill/

Course Logistics

Instructor: Adam O'Neill,
https://groups.cs.umass.edu/oneill/

take home

Grading: 3-5 homeworks (50%), ~~in class~~ midterm (25%), ~~in class~~ final exam (25%), may change final to course project if students prefer

take home

Course Logistics

Instructor: Adam O’Neill,
https://groups.cs.umass.edu/oneill/

Grading: 3-5 homeworks (50%), in-class midterm (25%), in-class final exam (25%), may change final to course project if students prefer

Graders: Dan Cline, Kunjal Panchal

Cryptography

Communication and computation (for data-at-rest) in the presence of an adversary

Cryptography

Communication and computation (for data-at-rest) in the presence of an adversary

An ancient art, *e.g.* Julius Caesar used cryptography

Cryptography

Communication and computation (for data-at-rest) in the presence of an adversary

An ancient art, *e.g.* Julius Caesar used cryptography

Transformed into a science starting with the work of Shannon (1949)

Cryptography

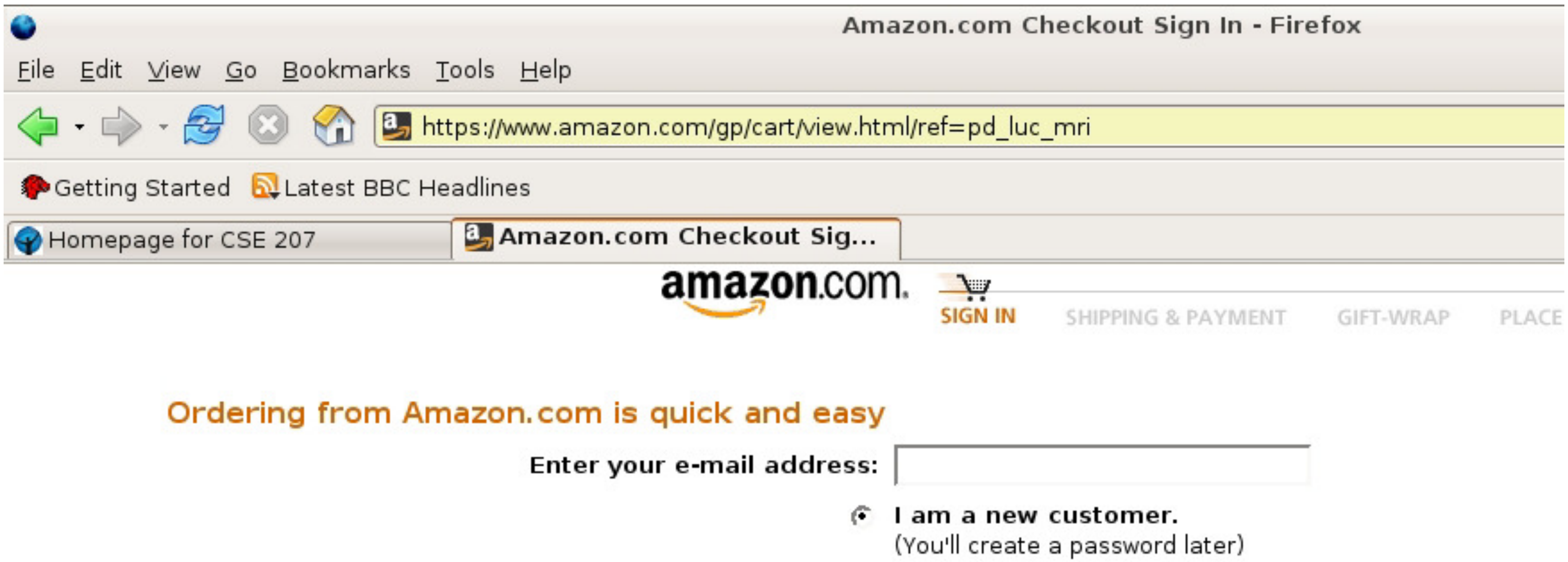
Communication and computation (for data-at-rest) in the presence of an adversary

An ancient art, *e.g.* Julius Caesar used cryptography

Transformed into a science starting with the work of Shannon (1949)

Took off in the 1970s and 1980s

Usage



- https invokes the TLS protocol
- TLS uses cryptography
- TLS is in ubiquitous use for secure communication: shopping, banking, Netflix, gmail, Facebook, ...

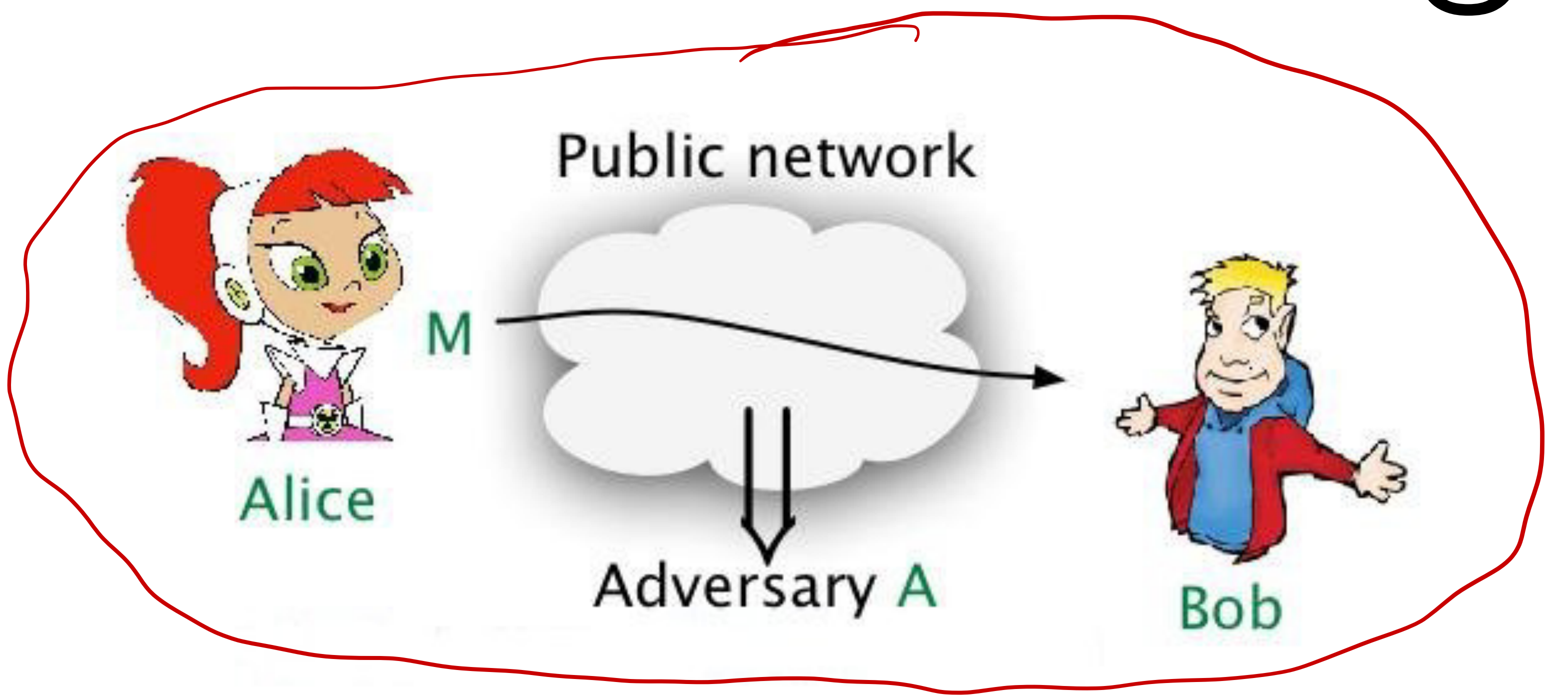
Other Uses

Other uses of cryptography:

- ATM machines
- Bitcoin
- Messaging apps: whatsapp, viber, line, telegraph, goldbug, chatsecure, ...
- Google authenticator
- ...

11,748 android apps use cryptography (encryption), and 10,327 get it wrong [EBFK13]

Classical Setting

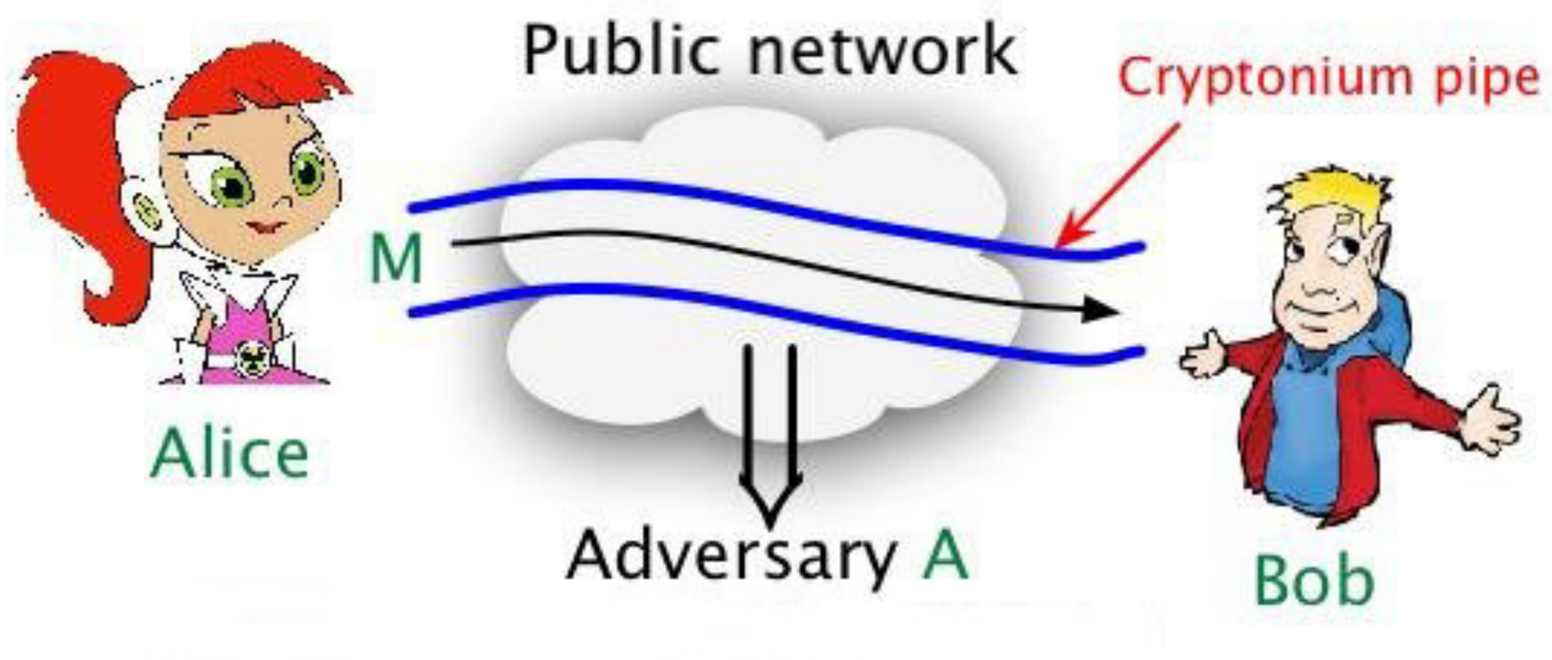


Adversary: clever person with powerful computer

Security goals:

- **Data privacy:** Ensure adversary does not see or obtain the data (message) M.
- **Data integrity and authenticity:** Ensure M really originates with Alice and has not been modified in transit.

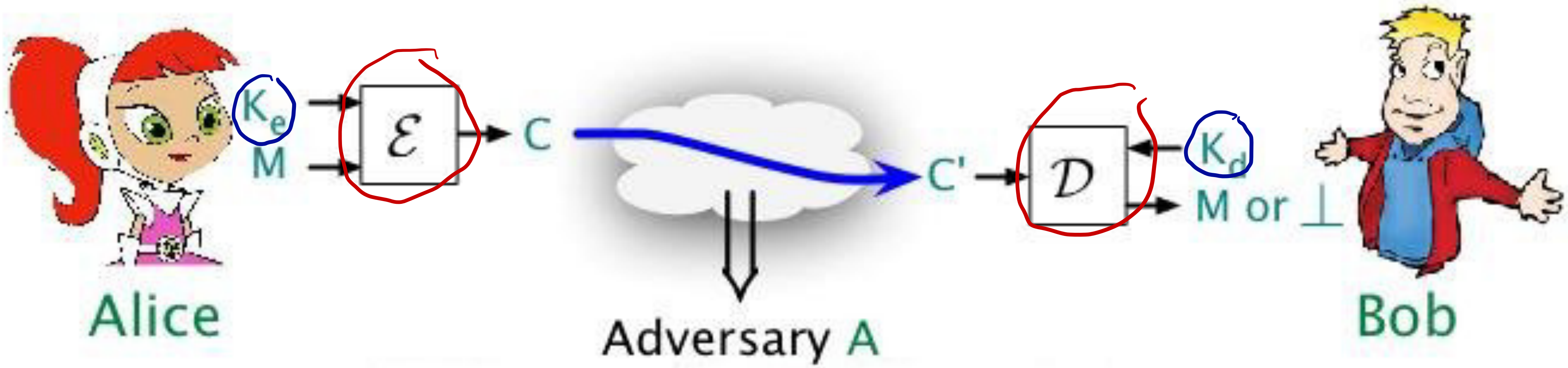
Ideal World



Cryptonium pipe: Cannot see inside or alter content.

All our goals would be achieved!

Cryptographic Schemes



$\mathcal{E}$: encryption algorithm $\quad$ K_e: encryption key

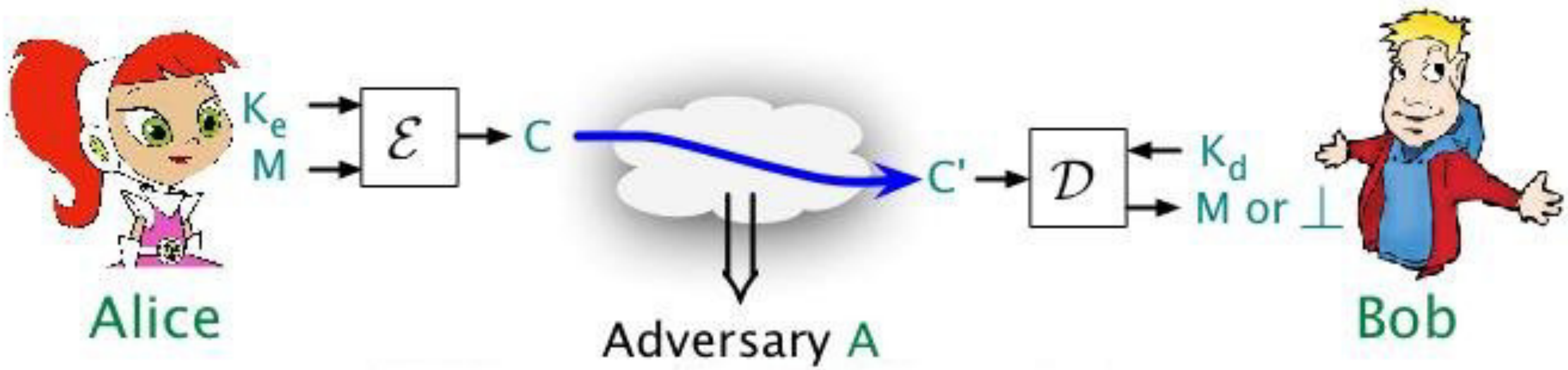
$\mathcal{D}$: decryption algorithm $\quad$ K_d: decryption key

Algorithms: standardized, implemented, public! ← Kerkoff's principle

$K_e = K_d$ symmetric encryption

$K_e \neq K_d$ public-key encryption

Settings



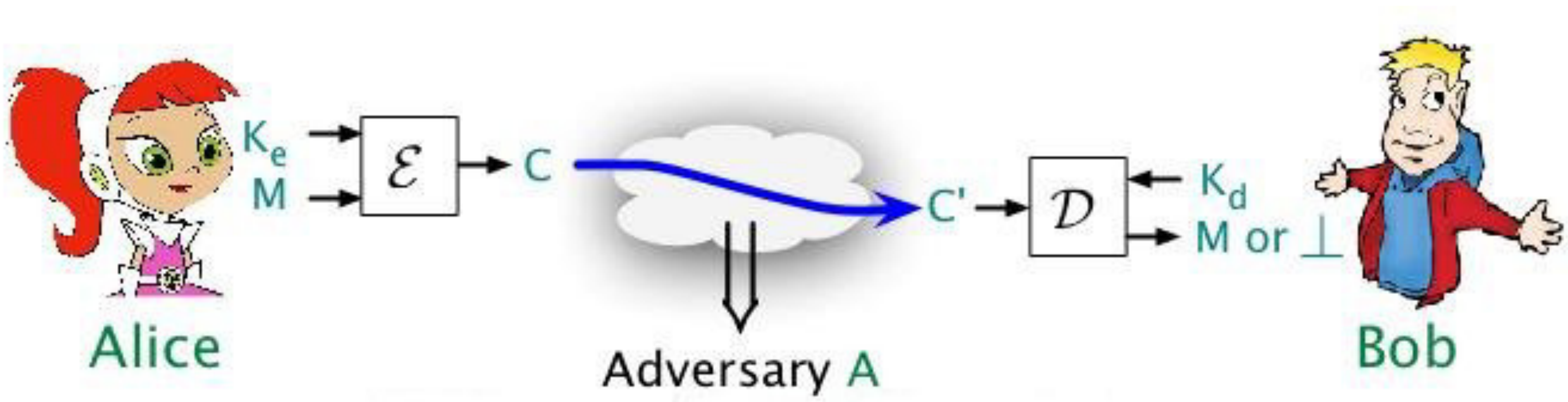
$\mathcal{E}$: encryption algorithm $\quad K_e$: encryption key

$\mathcal{D}$: decryption algorithm $\quad K_d$: decryption key

Settings:

- public-key (assymmetric): K_e public, K_d secret
- private-key (symmetric): $K_e = K_d$ secret

Key Distribution

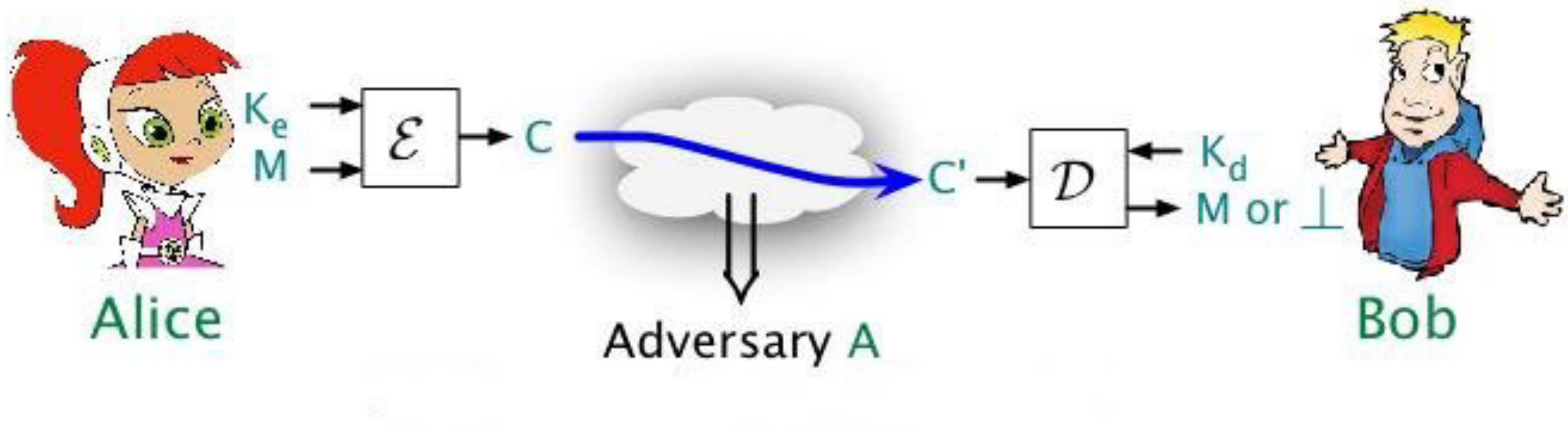


$\mathcal{E}$: encryption algorithm
$\mathcal{D}$: decryption algorithm

K_e: encryption key
K_d: decryption key

How do keys get distributed? Magic, for now!

Concerns



Our concerns:

- How to define security goals?
- How to design $\mathcal{E}$, $\mathcal{D}$?
- How to gain confidence that $\mathcal{E}$, $\mathcal{D}$ achieve our goals?

Why is this hard?

One cannot anticipate in advance what an adversary will do

Why is this hard?

One cannot anticipate in advance what an adversary will do

“Testing” is not possible in this setting

Why is this hard?

One cannot anticipate in advance what an adversary will do

“Testing” is not possible in this setting

Different than other areas of computer science where heuristics on “typical inputs” apply

Early History

Substitution ciphers/Caesar ciphers:

$$K_e = K_d = \pi \colon \Sigma \to \Sigma, \text{a secret permutation}$$

e.g., $\Sigma = \{A, B, C, \ldots\}$ and π is as follows:

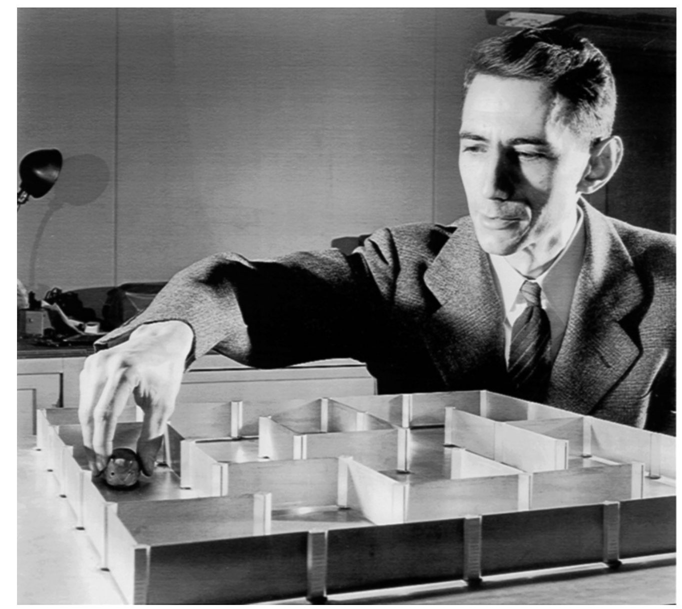
σ	A	B	C	D	$\cdots$
$\pi(\sigma)$	E	A	Z	U	$\cdots$

$$\begin{aligned} \mathcal{E}_\pi(CAB) &= \pi(C)\pi(A)\pi(B) \\ &= Z\ E\ A \\ \mathcal{D}_\pi(ZEA) &= \pi^{-1}(Z)\pi^{-1}(E)\pi^{-1}(A) \\ &= C\ A\ B \end{aligned}$$

Not very secure! (Common newspaper puzzle)

Shannon's Work

$$K_e = K_d = \underbrace{K \xleftarrow{\$} \{0,1\}^k}_{\substack{K \ \textit{chosen at random} \\ \textit{from } \{0,1\}^k}}$$



For any $M \in \{0,1\}^k$
- $\mathcal{E}_K(M) = K \oplus M$
- $\mathcal{D}_K(C) = K \oplus C$

Theorem (Shannon): OTP is perfectly secure as long as only one message encrypted.

"Perfect" secrecy, a notion Shannon defines, captures mathematical impossibility of breaking an encryption scheme.

$c_1 = K \oplus m_1 \qquad c_2 = K \oplus m_2$

$c_1 \oplus c_2 = m_1 \oplus m_2$

Information Theoretic Encryption

Notation

If S is a finite set then

$s \xleftarrow{\$} S$ sampling s at random from S.

If $\mathcal{D}_S$ is a distribution on S then

$s \xleftarrow{\$} \mathcal{D}_S$ sampling s according to $\mathcal{D}_S$.

$\Pr_{s \xleftarrow{\$} \mathcal{D}_S}[s = m]$ for som fixed $m \in S$.

Encryption

$(\mathcal{K}, \mathcal{E}, \mathcal{D})$ $\quad \mathcal{M}$ msg space

$K \xleftarrow{\$} \mathcal{K}$ outputs a random key.

$C \xleftarrow{\$} \mathcal{E}_K(m)$ outputs an enc. of m under K

$m \leftarrow \mathcal{D}_K(c)$ outputs a dec. of c under K

Correctness: $\forall m \in \mathcal{M} \quad \forall K \in \mathcal{K}$

$$\Pr_K[\mathcal{D}_K(\mathcal{E}_K(m)) = m]$$

is very large

Perfect Security

encryption deterministic

Definition 0.1. A cryptosystem $(\mathcal{K}, \mathcal{E}, \mathcal{D})$ is *perfectly secure* if for all distributions $\mathcal{D}$ on messages and every message g and every ciphertext c

"guess"

$$\Pr[\, g = m \mid \boxed{\mathcal{E}(K, m) = c} \,] = \Pr[\, \overset{g=m}{\cancel{m = g}} \,]$$

K, m

where the probability is over $K \leftarrow_{\$} \boxed{\mathcal{K}}$ and $m \leftarrow_{\$} \mathcal{D}$.

- Probabilities
- Distributions
- Random variables

R.V. $\boxed{K}$

outcome is in $\{0,1\}^k$

$\Pr[K = k] = \frac{1}{2^k}$

$D_K \sim U_K$

independent copies of r.v. K

Shannon Security

Definition 0.2. A cryptosystem $(\mathcal{K}, \mathcal{E}, \mathcal{D})$ is *Shannon secure* if for all messages m_0, m_1 and ciphertexts c

$$\Pr[\mathcal{E}(K, m_0) = c] = \Pr[\mathcal{E}(K, m_1) = c]$$

where the probability is over $K \leftarrow_\$ \mathcal{K}$.

$$\Updownarrow$$

$$\underline{E_K(m_0) \qquad E_K(m_1)}$$

$\forall m_0, m_1, K \xleftarrow{\$} \mathcal{K}$

"simpler formulation"

"handy"

An Equivalence

Theorem. A scheme is perfectly secure iff it is Shannon secure.

proof. (Shannon sec $\Rightarrow$ perfect)

Suppose $\Pr_{k}[E_k(m_0) = c] = \Pr_{k}[E_k(m_1) = c]$

WTS $\Pr_{k,m}[g = m \mid E_k(m) = c] = \Pr_{m}[g = m]$

$$\Pr[g=m \mid E_k(m)=c] = \frac{\Pr[g=m \wedge E_k(m)=c]}{\Pr[E_k(m)=c]}$$

$$= \frac{\Pr[g=m] \cdot \Pr[E_k(g)=c]}{\Pr[E_k(m)=c]}$$

(perfect sec. $\Rightarrow$ Shannon security)

Suppose $\Pr_{m,k}[m=g \mid E_k(m)=c] = \Pr[m=g]$

WTS $\Pr[E_k(m_0)=c] = \Pr[E_k(m_1)=c]$

$\forall m_0, m_1, c$

Let m_0, m_1 be arbitrary

Define $\mathcal{D} = \begin{cases} 1/2 & m_0 \\ 1/2 & m_1 \end{cases}$

$\Pr_{\mathcal{D}}[m = m_0 \mid E_k(m) = c] =$

$\Pr[\cancel{m = m_0}] \cdot \Pr[E_k(m_0) = c]$

$\Pr[E_k(m) = c]$

$\Pr_{\mathcal{D}}[\cancel{m = m_0}]$

$\frac{1}{2}$

$\Pr[E_k(m_0) = c] = \cancel{1}$

$\Pr[E_k(\cancel{m}) = c]$

$= \Pr[E_k(m_1) = c]$

$\Pr[E_k(\cancel{m}) = c]$

by perfect sec.

- decryption error

- $\Pr[E_K(m_0) = c]$ is close to $\Pr[E_K(m_1) = c]$

Shannon's Theorem

Theorem. For Shannon security keys need to be as long as messages.

$$\forall c \ \exists K \quad D_K(c) = m$$

$$\forall m$$

$c, m^*, m \qquad \Pr[E_K(m^*) = c]$

$$\neq \Pr[E_K(m) = c]$$

Statistical Indistinguishability

$X = E_k(m_0) \quad Y = E_k(m_1)$

$$\Delta(X,Y) = \frac{1}{2}\sum_x \left| \Pr[X=x] - \Pr[Y=x] \right|$$

measure of closeness between two r.v.'s

Statistical distance

indistinguishability

$$\max_A \left| \Pr[A(X) \Rightarrow 1] - \Pr[A(Y) \Rightarrow 1] \right| = \Delta(X,Y)$$

X, Y are ε-indistinguishable

OTP

Modern Cryptography

Gets around Shannon's Theorem by developing a computational science

Modern Cryptography

Gets around Shannon's Theorem by developing a computational science

Security of a practical scheme must rely not on impossibility but on computational intractability

Modern Cryptography

Gets around Shannon's Theorem by developing a computational science

Security of a practical scheme must rely not on impossibility but on computational intractability

Not only of imminent practical value, cryptography is full of counter-intuitive solutions to cool problems!

Security Theorems

Rather than:

> *"It is impossible to break the scheme"*

We might be able to say:

> *"No attack using $\leq 2^{160}$ time succeeds with probability $\geq 2^{-20}$"*

I.e., Attacks can exist as long as cost to mount them is prohibitive, where Cost = computing time/memory, $$$