Lecture 1. Introduction

Definitions and one-time pad

Bruno Grenet

https://membres-ljk.imag.fr/Bruno.Grenet/IntroCrypto.html

Introduction to cryptology
Université Grenoble Alpes – IM²AG
M1 INFO, MOSIG & AM

Administrativia

Lectures / tutorial sessions

- 1 lecture and 1 tutorial session per week
  - Fridays, in French with Bruno Grenet — M1 INFO
  - Thursdays, in English with Léo Colisson Palais — M1 Mosig/AM
- Practical sessions: twice in the semester, replacing the tutorial session

Exams

- Mid-term in-class exam, ~1.5h — date to be fixed
- Final in-class exam, 2h — tentative date: April 27.
  - If needed: retake exam, 2h — tentative date: July 2.
- Grade:
  1. *Première session*: $0.3 \times \text{MidTerm} + 0.7 \times \text{Final}$
  2. *Deuxième session*: $\max(\text{Retake}; 0.3 \times \text{MidTerm} + 0.7 \times \text{Retake})$

Website: https://membres-ljk.imag.fr/Bruno.Grenet/IntroCrypto.html

- All the (annotated) slides, exercise sheets, past exams, some extra writings
- Some recommended textbooks — none required!

What is cryptography?

Protecting secret data from adversaries

- Communications — email, web, credit card payment, …
- Storage — encrypted hard drive, …
- Computations — electronic voting, …
- …

Used with various hardware

- High-end CPUs, mobile phones, microcontrollers, dedicated hardware
- Varying speed (throughput & latency), code/circuit size, energy consumption, …

"Doing crypto"

- Designing new primitives, constructions, protocols, …
- Analysing existing primitives, …
- Deploying crypto in products — incl. implementation

Historical ciphers

- Shift ciphers — *Caesar (50 BC); `rot13`*
- Substitution ciphers — *Atbash (600-500 BC)*
- Transposition ciphers — *Scytale (400 BC)*
- Polyalphabetic cipher — *Vigenère (1553); Enigma (1920s)*
- …

None of them is safe!

- Attacks: brute force, frequency analysis (1863), bombe (1938-40), …
- Some lessons drawn:
  - Large enough *key space* is needed
  - Designing an encryption system is *difficult*
  - Assessing its security is (even more?) difficult

Modern cryptography

What does it mean to be *secure*?

Defining security

Achieve some *goals*

- Confidentiality — *no adversary can read the data*
- Proof of identity — *that's me!*
- Authenticity — *no adversary can impersonate the sender*
- Integrity — *no adversary can modify the data*
- …

In the presence of *adversaries*

- Passive adversary — *eavesdropper*
- Active adversary — *can modify messages exchanged*

With or without *shared secret*

- Large — *one-time pad*
- Small — *symmetric cryptography*
- None — *public-key cryptography*

Defining security

Achieve some *goals*

- Confidentia *can read the data*
- Proof of ide *that's me!*
- Authenticit *sonate the sender*
- Integrity *modify the data*
- …

In the presence

- Passive adv *eavesdropper*
- Active adve *ssages exchanged*

With or withou

- Large *one-time pad*
- Small *symmetric cryptography*
- None *public-key cryptography*

https://xkcd.com/538/

The big picture of this course

	small shared secret symmetric cryptography	no shared secret public-key cryptography
passive adversaries confidentiality	*symmetric encryption*	*public-key encryption*
active adversaries authenticity	*message authentication codes*	*digital signatures*
active adversaries confidentiality+authenticity	*authenticated encryption*	*signcryption*

Other constructions

- *Key exchange* — agree on a secret in presence of passive adv.
- *Hybrid encryption* — combine symmetric and public-key crypto.
- *Hash functions*

Not in the course

- Implementations, use of cryptographic softwares and libraries, …

Course contents

Lectures

1.	Introduction	*One-time pad*
2.	Block ciphers	*AES*, *DES*
3.	Symmetric encryption	*CBC* & *CTR* modes of operation
4.	Hash functions	*SHA-2*, *SHA-3*
5.	Messages authentication codes & authenticated encryption	*CBC-MAC*, *HMAC*, *GCM*
6.	Key exchange	*Diffie-Hellman*
7.	Public-key encryption & key encapsulation	*ElGamal*
8.	Signatures	*Schnorr*, *DSA*
9.	RSA	
10.	Putting it all together	*TLS*

Common topics

- Definitions and security notions
- Proofs of security
- Examples & attacks

Contents

1. A first example: the one-time pad

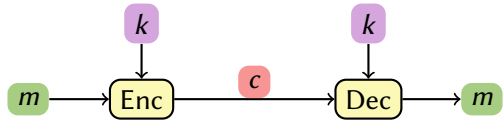
2. IND-CPA security

Contents

1. A first example: the one-time pad

2. IND-CPA security

Vocabulary of (symmetric) encryption



- m message *or* plaintext
- c ciphertext
- k key
- Enc $\mathcal{K} \times \mathcal{M} \to \mathcal{C}$ is the encryption algorithm
- Dec $\mathcal{K} \times \mathcal{C} \to \mathcal{M}$ is the decryption algorithm

$\mathcal{M}$: message space
$\mathcal{C}$: ciphertext space
$\mathcal{K}$: key space
$\text{Enc}_k(m)$
$\text{Dec}_k(m)$

Correctness

$\Sigma = (\text{Enc}, \text{Dec})$ is correct if for any $m \in \mathcal{M}$ and $k \in \mathcal{K}$, $\text{Dec}_k(\text{Enc}_k(m)) = m$

The one-time pad

Input: *Message* $m \in \{0,1\}^\lambda$ (or *plaintext*)
Secret: Key $k \in \{0,1\}^\lambda$
Output: *Ciphertext* $c \in \{0,1\}^\lambda$

message space: $\mathcal{M} = \{0,1\}^\lambda$
key space: $\mathcal{K} = \{0,1\}^\lambda$
ciphertext space: $\mathcal{C} = \{0,1\}^\lambda$

Algorithms

Encryption: $\mathsf{Enc}_k(m) = m \oplus k$
Decryption: $\mathsf{Dec}_k(c) = c \oplus k$

$m = 010011$
$k = 110001$
$c = 100010$
$\lambda = 6$

Lemma

The one-time pad is *correct*: $\forall k \in \mathcal{K}, \forall m \in \mathcal{M}, \mathsf{Dec}_k(\mathsf{Enc}_k(m)) = m$

Proof

$\forall k,\ k \oplus k = 0^\lambda$ and $\forall m,\ m \oplus 0^\lambda = m$

$\mathsf{Dec}_k(\mathsf{Enc}_k(m)) = (m \oplus k) \oplus k = m \oplus k \oplus k = m$

Security for the one-time pad

Tentative definition

Given $c = \mathrm{Enc}_k(m)$, it is *impossible* to find m without knowing k

What does *impossible* mean?

- Probability of guessing m is at least $1/2^\lambda$

Is this enough?

- What if an adversary learns k?
- What if an adversary learns one bit of m?
- What if an adversary learns $\bigoplus_i m_{[i]}$? *xor of all bits*
- What if an adversary learns that $m \in \{0011, 0101, 1000\}$?

Security for the one-time pad

~~Tentative definition~~

~~Given $c = \mathrm{Enc}_k(m)$, it is *impossible* to find m~~

What does *impossible* mean?

- Probability of guessing m is at least $1/2^\lambda$

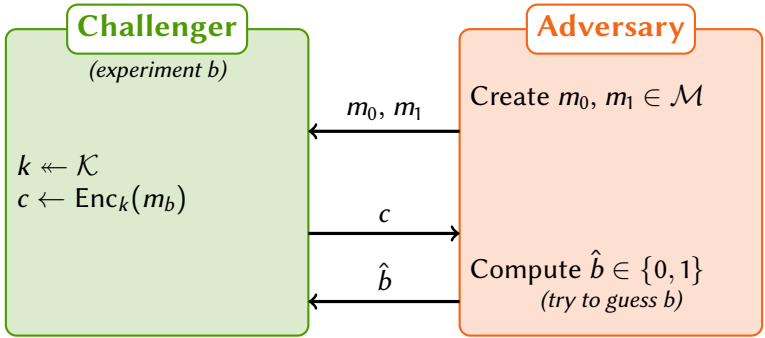
Is this enough?

- What if an adversary learns k?
- What if an adversary learns one bit of m?
- What if an adversary learns $\bigoplus_i m_{[i]}$? *xor of all bits*
- What if an adversary learns that $m \in \{0011, 0101, 1000\}$?

Better definition

The ciphertext should provide no (extra) information about the message to an adversary

The *perfect indistinguishability* game



Informal definitions

Enc is *perfectly indistinguishable* if

- the adversary has probability $\frac{1}{2}$ to correctly guess b *win the game*
- the adversary has the same behavior, whether $b = 0$ or $b = 1$

Notation $x \twoheadleftarrow S$: x sampled uniformly at random from S

Perfect indistinguishability

a.k.a information-theoretic security *or* unconditional security

Definition

Enc is *perfectly indistinguishable* if $\Pr\left[\mathcal{A}^{\mathsf{Enc}_k} \to 1 \middle| b = 0\right] = \Pr\left[\mathcal{A}^{\mathsf{Enc}_k} \to 1 \middle| b = 1\right]$

(probability taken over the random choice for *k and whatever randomness is used by the Adversary*)

Be careful!

- In both experiments, probability that the adversary outputs 1
  - "prob. of failure in exp. 0 = prob. of success in exp. 1"
- The adversary has the same behavior, whatever the value of b
  - It has no information on b

Equivalent definitions

- If the challenger samples $b \twoheadleftarrow \{0,1\}$ and runs experiment b, $\Pr\left[\hat{b} = b\right] = \frac{1}{2}$
- For every $m_0, m_1 \in \mathcal{M}$, $c \in \mathcal{C}$, if $k \twoheadleftarrow \mathcal{K}$, $\Pr[c = \mathsf{Enc}_k(m_0)] = \Pr[c = \mathsf{Enc}_k(m_1)]$

Perfect indistinguishability

a.k.a information-theoretic security *or* unconditional security

Definition

Enc is *perfectly indistinguishable* if $\Pr\left[\mathcal{A}^{\mathsf{Enc}_k} \to 1 \middle| b = 0\right] = \Pr\left[\mathcal{A}^{\mathsf{Enc}_k} \to 1 \middle| b = 1\right]$

(probability taken over the random choice for k *and whatever randomness is used by the Adversary*)

Be careful!

- In both experiments, probability that the adversary outputs 1
  - ~~"prob. of failure in exp. 0 = prob. of success in exp. 1"~~
- The adversary has the same behavior, whatever the value of b
  - It has no information on b

Equivalent definitions

- If the challenger samples $b \twoheadleftarrow \{0,1\}$ and runs experiment b, $\Pr\left[\hat{b} = b\right] = \frac{1}{2}$
- For every $m_0, m_1 \in \mathcal{M}$, $c \in \mathcal{C}$, if $k \twoheadleftarrow \mathcal{K}$, $\Pr[c = \mathsf{Enc}_k(m_0)] = \Pr[c = \mathsf{Enc}_k(m_1)]$

Consequences of perfect indistinguishability

Lemma

Given $c \leftarrow \mathrm{Enc}_k(m)$, no adversary can learn

(i) the least significant bit $m_{[0]}$ of m
(ii) the value of k
(iii) the parity $\bigoplus_{i=0}^{\lambda-1} m_{[i]}$ of m
(iv) whether $m \in \{0011, 0101, 1000\}$
(v) …

Proof of (i)

Assume $\mathcal{A}$ is able to learn $m_{[0]}$, given $c \leftarrow \mathrm{Enc}_k(m)$.

We use $\mathcal{A}$ in the perfect ind. game:

- $\mathcal{A}_0$ creates $m_0 = 0^1$ and $m_1 = 1^1$
- When $\mathcal{A}$ receives c, it computes $m_{b[0]}$ and outputs $\hat{b} = m_{b[0]}$

$\Pr[\mathcal{A}^{\mathrm{Enc}_k} \to 1 \mid b=0] = 0 \neq \Pr[\mathcal{A}^{\mathrm{Enc}_k} \to 1 \mid b=1] = 1 \Rightarrow$ Enc is not perf. ind.

Security of one-time pad encryption

Theorem

The one-time pad is perfectly indistinguishable

Proof

- Lemma For any $m \in \mathcal{M}$ and $c \in \mathcal{C}$, $\Pr_{k \leftarrow \mathcal{K}}[m \oplus k = c] = 1/2^n$

  If $\Pr_k[m \oplus k = c] = \Pr_k[\underbrace{m \oplus c}_{\text{fixed} \in \{0,1\}^n} = k] = 1/2^n$ ☒

- Assume that A is deterministic: we can define $\mathcal{C}_1 \subset \mathcal{C}$ s.t. $A^{\text{Enc}_k} \to 1$ when $c \in \mathcal{C}_1$. $\Pr_k[A^{\text{Enc}_k} \to 1] = \Pr[c \in \mathcal{C}_1] = \frac{\#\mathcal{C}_1}{2^n}$

  Here b plays no role, so $\Pr[A^{\text{Enc}_k} \to 1 \mid b=0] = \Pr[A^{\text{Enc}_k} \to 1 \mid b=1] = \frac{\#\mathcal{C}_1}{2^n}$

Security of one-time pad encryption

Theorem

The one-time pad is perfectly indistinguishable

Proof

- Assume now that A is randomized.

Let $r \in \{0,1\}^*$ be the random bits used by A.

For any $r \in \{0,1\}^*$, let A_r be the deterministic adversary obtained by fixing these bits.

law of total probabilities

$$\Pr\left[A^{\mathrm{Enc}_k} \to 1\right] = \sum_{r \in \{0,1\}^*} \Pr\left[A_r^{\mathrm{Enc}_k} \to 1\right] \Pr\left[A \text{ used } r \text{ as random bits}\right]$$

↳ Since this does not depend on b, $\Pr\left[A^{\mathrm{Enc}_k} \to 1 \mid b=0\right] = \Pr\left[A^{\mathrm{Enc}_k} \to 1 \mid b=1\right]$

Conclusion on one-time pad

Pros

- Used during the cold war
- Used for small plaintexts/secrets
- Perfectly secret/indistinguishable

Cons & caveats

- Key as long as the message
- Can be used only once
- The key must be uniformly sampled

Shannon's theorem

A *perfectly indistinguishable* encryption scheme must satisfy:

(i) $\#\mathcal{K} \geq \#\mathcal{M}$

(ii) if $\#\mathcal{K} = \#\mathcal{M}$, k must be uniformly sampled from $\mathcal{K}$

Conclusion on one-time pad

Pros
- ▶
- ▶
- ▶

led

Sha

A *p*

(i)

(ii)

Proof of (i). Perfect ind. $\Rightarrow \#\mathcal{K} \geq \#\mathcal{T}$

- Assume $\#\mathcal{K} < \#\mathcal{T}$. For $c \in \mathcal{C}$, define $\mathcal{T}_c = \{m : \mathrm{Dec}_k(c) = m \text{ for some } k \in \mathcal{K}\}$
- Since the decryption is deterministic, $\#\mathcal{T}_c \leq \#\mathcal{K} < \#\mathcal{T}$
- Take $c^* \in \mathcal{C}$ s.t. $\mathcal{T}_{c^*} \neq \emptyset$ and $m_0 \in \mathcal{T}_{c^*}$, $m_1 \in \mathcal{T} \setminus \mathcal{T}_{c^*}$.
- $\mathcal{A}$ sends m_0 and m_1
  If $\mathcal{A}$ receives c^*, it outputs $\hat{b} = 0$
  Otherwise, $\mathcal{A}$ outputs a random bit $\hat{b}$

$$\left.\begin{array}{l} \Pr\left[\mathcal{A}^{\mathrm{Enc}_k} \to 1 \mid b=0\right] = \\ \quad 0 \times \Pr[c = c^*] + \frac{1}{2}\Pr[c \neq c^*] \\ \Pr\left[\mathcal{A}^{\mathrm{Enc}_k} \to 1 \mid b=1\right] = \frac{1}{2} \end{array}\right\}$$

↳ Enc is not perf. ind.

Conclusion on one-time pad

Pros

- Used during the cold war
- Used for small plaintexts/secrets
- Perfectly secret/indistinguishable

Cons & caveats

- Key as long as the message
- Can be used only once
- The key must be uniformly sampled

Shannon's theorem

A *perfectly indistinguishable* encryption scheme must satisfy:

(i) $\#\mathcal{K} \geq \#\mathcal{M}$

(ii) if $\#\mathcal{K} = \#\mathcal{M}$, k must be uniformly sampled from $\mathcal{K}$

One-time pad is insufficient

- Encryption schemes with smaller keys / that allow to *reuse* a key
- Relaxation of the security notion

Contents

1. A first example: the one-time pad

2. IND-CPA security

Principles of modern cryptography

Formal definitions

- What does *secure encryption* mean?
  - An adversary cannot recover the key
  - An adversary cannot recover the message from the ciphertext
  - An adversary cannot retrieve any character of the message from the ciphertext
  - …

Principles of modern cryptography

Formal definitions

- What does *secure encryption* mean?
  - (good definition) Whatever information an adversary has about the message, the ciphertext only provides them with *very little* additional information

Principles of modern cryptography

Formal definitions

- What does *secure encryption* mean?
  - (good definition) Whatever information an adversary has about the message, the ciphertext only provides them with *very little* additional information
- What is an *adversary*?
  - Assumptions on the information it has access to
  - Assumptions on its computational power complexity theory

Principles of modern cryptography

Formal definitions

- What does *secure encryption* mean?
  - (good definition) Whatever information an adversary has about the message, the ciphertext only provides them with *very little* additional information
- What is an *adversary*?
  - Assumptions on the information it has access to
  - Assumptions on its computational power — complexity theory

Kerckhoff's principle

The adversary knows the details of the protocol, but not the secret used

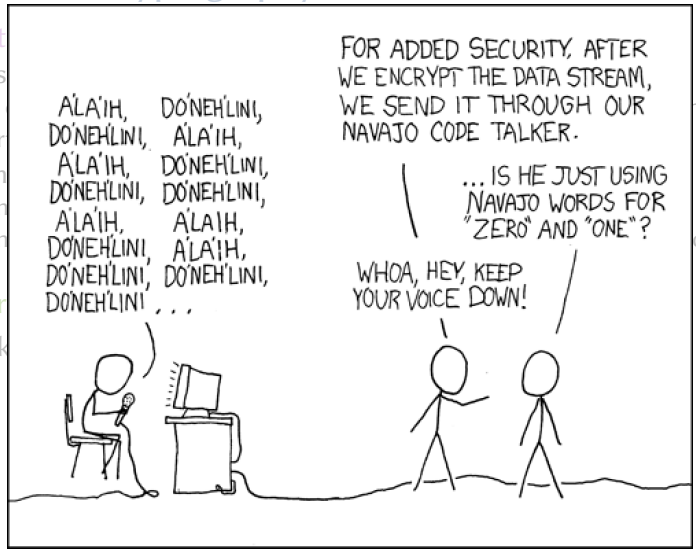
Principles of modern cryptography

Formal definit

- What does
  - (good
    cipher
- What is an
  - Assum
  - Assum

Kerckhoff's pr

The adversary k



https://xkcd.com/257/

Principles of modern cryptography

Formal definitions

- What does *secure encryption* mean?
  - (good definition) Whatever information an adversary has about the message, the ciphertext only provides them with *very little* additional information
- What is an *adversary*?
  - Assumptions on the information it has access to
  - Assumptions on its computational power — complexity theory

Kerckhoff's principle

The adversary knows the details of the protocol, but not the secret used

Provable security

- *Proving* that a protocol satisfies a *security definition*, assuming *assumptions*
- Study of assumptions: validity, necessity, comparisons

Towards a good security notion

Perfect indistinguishability is not suitable

- Too strong: No matter how powerful, an adversary learns nothing
- Too weak:
  - The adversary only sees one ciphertext
  - No guarantee if a key is reused

Relax

- Allow the adversary to distinguish with *very low* probability
- Only consider *computationally bounded* adversaries

Strengthen

- Ciphertext-only attack — COA
- Known-plaintext attack — KPA
- Chosen-plaintext attack — CPA
- Chosen-ciphertext attack — CCA

Towards a good security notion

Perfect indistinguishability is not suitable

- Too strong: No matter how powerful, an adversary learns nothing
- Too weak:
  - The adversary only sees one ciphertext
  - No guarantee if a key is reused

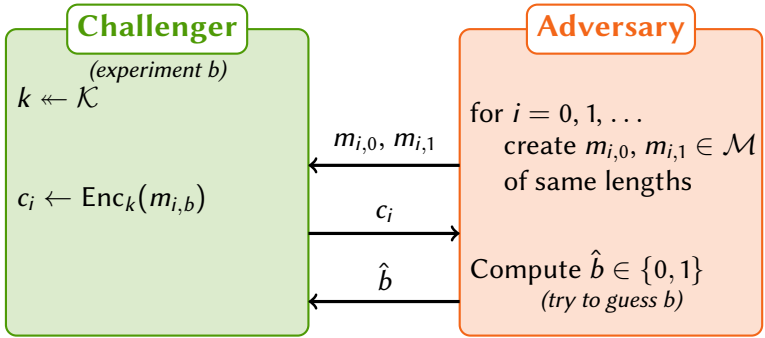
Relax

- Allow the adversary to distinguish with *very low* probability
- Only consider *computationally bounded* adversaries

Strengthen

- ~~Ciphertext-only attack~~ ~~COA~~
- ~~Known-plaintext attack~~ ~~KPA~~
- Chosen-plaintext attack CPA
- Chosen-ciphertext attack CCA

IND-CPA Game



Comparison with perfect indistinguishability

- Several pairs of messages, encrypted with the same key *chosen plaintext attack*
  - query $m_{i,0} = m_{i,1} \rightarrow$ encryption of $m_{i,0}$
- Attack against one-time pad:
  - query $m_{0,0} = m_{0,1} = 0^\lambda \rightarrow c_0 = 0^\lambda \oplus k = k$
  - query $m_{1,0} \neq m_{1,1} \rightarrow$ decrypt c_1 with k

IND-CPA *advantage*

Definition

$$\mathrm{Adv}_{\mathrm{Enc}}^{\text{IND-CPA}}(\mathcal{A}) = \left| \Pr\left[\mathcal{A}^{\mathrm{Enc}_k} \to 1 | b = 0\right] - \Pr\left[\mathcal{A}^{\mathrm{Enc}_k} \to 1 | b = 1\right] \right|$$

- value between 0 ($\mathcal{A}$ has no information on b) and 1 ($\mathcal{A}$ finds b)
- *advantage* compared to sampling $\hat{b}$ uniformly at random

Lemmas

- If Enc is deterministic, $\exists \mathcal{A}$ with advantage 1 *cf.* attack on one-time pad
- An adversary with *unbounded power* has advantage 1:

What is an *adversary*?

An adversary is a randomized algorithm

Why an algorithm?

- Slightly generalized: several interactions with the challenger — *oracle* / *black box*
  - query $(m_{i,0}, m_{i,1}) \to$ response c_i, $i \geq 0$
  - eventually outputs $\hat{b}$
- A clever human adversary can be modelled by an algorithm

Why randomized?

- Why assume that the adversary does not call `random()`?
- More general adversaries — not in this course
  - side channel attack: access to internal states of the challenger
  - quantum algorithm — *post-quantum cryptography*

The IND-CPA security

IND-CPA secure: **any** *efficient* adversary has *negligible* advantage

Security parameter

- $\Sigma = (\mathsf{Enc}, \mathsf{Dec})$ is a *family of encryption schemes*
  - parameterized by a *security parameter* λ…
  - … that defines the key size $\mathcal{K}$ depends on λ
- $\mathsf{Adv}^{\text{IND-CPA}}_{\mathsf{Enc}}(\mathcal{A})$ usually depends on λ

Advantage function

$$\mathsf{Adv}^{\text{IND-CPA}}_{\mathsf{Enc}}(q, t) = \max_{\mathcal{A}_{q,t}} \mathsf{Adv}^{\text{IND-CPA}}_{\mathsf{Enc}}(\mathcal{A}_{q,t})$$

(the max is taken over all adversaries $\mathcal{A}_{q,t}$ that perform $\leq q$ queries and $\leq t$ operations)

- The advantage function should be *negligible* for *bounded* q and t

Two approaches

IND-CPA secure: **any** *efficient* adversary has *negligible* advantage

Asymptotic security

complexity-theoretic definition

- Expressed in terms of the *security parameter* λ
- Efficient: polynomial in λ $\qquad q = \mathrm{poly}(\lambda),\ t = \mathrm{poly}(\lambda)$
- Negligible: $< 1/p(\lambda)$ for any polynomial p

$$\text{Enc is IND-CPA secure} \iff \mathrm{Adv}^{\text{IND-CPA}}_{\text{Enc}}(\mathrm{poly}(\lambda), \mathrm{poly}(\lambda)) \ll 1/\mathrm{poly}(\lambda)$$

Concrete security

mostly chosen in this course

- No formal definition of *efficient* or *negligible*
- Compare schemes by comparing their advantage functions
- Plug some explicit values:
  - what is an *reasonable* number of operations / number of queries?
  - what is an *acceptable* advantage?

Orders of magnitude (time)

Computation time: number of elementary operations

- $t \simeq 2^{40}$: $\sim$ 1 day on my laptop
- $t \simeq 2^{60}$: possible on a large CPU/GPU cluster — done in academia
- $t \simeq 2^{80}$: possible with an ASIC cluster — Bitcoin mining
- $t \simeq 2^{128}$: *very* hard

How much time for 2^{128} operations?

- With all 500 fastest super-computers, assuming parallelizability — $10 \cdot 10^9$ gFLOPS
- Time: $2^{128}/(10 \cdot 10^9 \cdot 10^9 \times 365 \cdot 24 \cdot 3600) \approx 10^{12}$ years — $\approx 4\times$ age of Earth

How much power for 2^{128} operations in 100 years?

- With hardware at 10^6 gFLOPS using 1 000W per device — pretty good!
- Number of devices: $2^{128}/(10^6 \cdot 10^9 \times 100 \cdot 365 \cdot 24 \cdot 3600) \approx 10^{14}$
- Power: $10^{14} \times 1000\text{W} \approx 100\,000$ TW — $\approx 65 \cdot 10^6$ EPR

Orders of magnitude (probabilities)

Probabilities

- $p = \frac{1}{2}$: get a TAIL with a fair coin
- $p = \frac{1}{6}$: get a 6 with a fair die
- $p \approx 2^{-24}$: probability to win at French lottery
- $p \approx 2^{-72}$: probability to win 3 times in a row at French lottery

Examples

- An attack that takes 1 second and has a probability of success of 2^{-60} is expected to have succeeded less than once since the Big Bang
- Errors in CPU due to cosmic rays happen with much larger probabilities!

Combining orders of magnitude

If $\mathsf{Adv}^{\text{IND-CPA}}_{\text{Enc}}(2^{128}, 2^{128}) < 2^{-60}$, Enc is pretty (IND-CPA) secure!

Orders of magnitude (probabilities)

Probabilities

- $p = \frac{1}{2}$: get a TAIL with a fa
- $p = \frac{1}{6}$: get a 6 with a fair c
- $p \approx 2^{-24}$: probability to w
- $p \approx 2^{-72}$: probability to w

h lottery

Examples

- An attack that takes 1 sec
- Errors in CPU due to cosm

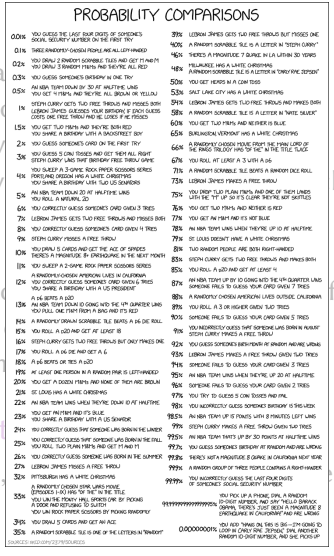
f success of 2^{-60} is expected to have succeeded less than

larger probabilities!

Combining orders of magnit

If $\mathrm{Adv}^{\mathrm{IND\text{-}CPA}}_{\mathrm{Enc}}(2^{128}, 2^{128}) < 2^{-60}$,

cure!



https://xkcd.com/2379/

17%	YOU ROLL A D6 DIE AND GET A 6
18%	A D6 BEATS OR TIES A D20
19%	AT LEAST ONE PERSON IN A RANDOM PAIR IS LEFT-HANDED
20%	YOU GET A DOZEN M&MS AND NONE OF THEM ARE BROWN
21%	ST. LOUIS HAS A WHITE CHRISTMAS
22%	AN NBA TEAM WINS WHEN THEY'RE DOWN 10 AT HALFTIME
23%	YOU GET AN M&M AND IT'S BLUE YOU SHARE A BIRTHDAY WITH A US SENATOR
24%	YOU CORRECTLY GUESS THAT SOMEONE WAS BORN IN THE WINTER
25%	YOU CORRECTLY GUESS THAT SOMEONE WAS BORN IN THE FALL YOU ROLL TWO PLAIN M&MS AND GET M AND M
26%	YOU CORRECTLY GUESS SOMEONE WAS BORN IN THE SUMMER
27%	LEBRON JAMES MISSES A FREE THROW
32%	PITTSBURGH HAS A WHITE CHRISTMAS
33%	A RANDOMLY CHOSEN STAR WARS MOVIE (EPISODES I-IX) HAS "OF THE" IN THE TITLE YOU WIN THE MONTY HALL SPORTS CAR BY PICKING A DOOR AND REFUSING TO SWITCH YOU WIN ROCK PAPER SCISSORS BY PICKING RANDOMLY
34%	YOU DRAW 5 CARDS AND GET AN ACE
35%	A RANDOM SCRABBLE TILE IS ONE OF THE LETTERS IN "RANDOM"

93%	LEBRON JAMES MAKES A FREE THROW GIVEN TWO TRIES
94%	SOMEONE FAILS TO GUESS YOUR CARD GIVEN 3 TRIES
95%	AN NBA TEAM WINS WHEN THEY'RE UP 20 AT HALFTIME
96%	SOMEONE FAILS TO GUESS YOUR CARD GIVEN 2 TRIES
97%	YOU TRY TO GUESS 5 COIN TOSSES AND FAIL
98%	YOU INCORRECTLY GUESS SOMEONE'S BIRTHDAY IS THIS WEEK
98.5%	AN NBA TEAM UP 15 POINTS WITH 8 MINUTES LEFT WINS
99%	STEPH CURRY MAKES A FREE THROW GIVEN TWO TRIES
99.5%	AN NBA TEAM THAT'S UP BY 30 POINTS AT HALFTIME WINS
99.7%	YOU GUESS SOMEONE'S BIRTHDAY AT RANDOM AND ARE WRONG
99.8%	THERE'S NOT A MAGNITUDE 8 QUAKE IN CALIFORNIA NEXT YEAR
99.9%	A RANDOM GROUP OF THREE PEOPLE CONTAINS A RIGHT-HANDER
99.99%	YOU INCORRECTLY GUESS THE LAST FOUR DIGITS OF SOMEONE'S SOCIAL SECURITY NUMBER
99.999999999999995%	YOU PICK UP A PHONE, DIAL A RANDOM 10-DIGIT NUMBER, AND SAY "HELLO BARACK OBAMA, THERE'S JUST BEEN A MAGNITUDE 8 EARTHQUAKE IN CALIFORNIA!" AND ARE WRONG
0.000000001%	YOU ADD "HANG ON, THIS IS BIG—I'M GOING TO LOOP IN CARLY RAE JEPSEN," DIAL ANOTHER RANDOM 10-DIGIT NUMBER, AND SHE PICKS UP

SOURCES: XKCD.COM/2379/SOURCES

https://xkcd.com/2379/

Summary

One-time pad

- Very important primitive
  - used as a building block within larger protocols
  - used as a goal: try to mimic the one-time pad with smaller keys
- Not usable per se in practice
  - Key as large as the message
  - Never reuse the key!

Game-based security definition

- Adversary plays against a Challenger, with
  - a goal — *e.g.* indistinguishability (IND)
  - some means — *e.g.* chosen plaintext attack (CPA)
- Advantage: how better than randomly guessing?
- Computational security: the advantage is *negligible* for any *efficient* adversary

Going further

Other security definitions

- Stronger goal: non-malleability — active adversary
- Stronger means: chosen ciphertext attack (CCA)
- Non game-based definitions: composable / simulation-based security
- Beyond encryption: security notions for authenticity, …

What's next?

- Symmetric and public-key encryption
- Authentication and integrity
- Pseudo-random permutations, hash functions, …
- Each time:
  - What is the suitable security notion?
  - How to achieve this security notion?

Recap on probability theory on the webpage

- Introduction to discrete probabilities
- B. Barak, *An Intensive Intro. to Cryptography*. Chap. 0. Math. background