Lecturer: Michael J May
Kinneret Academic College

Electronic Security, Requirements, Cryptographic Foundations, One time pads

20 March 2025

Lecture 1

Course Topic: Security!

- Our goal is to gain an understanding of the tools and techniques of modern digital communication security
- This is an introductory course!

- What you won't learn:
  - How to hack into a misconfigured Apache web server
  - How to write viruses
  - Why web sites and Java have so many bugs
  - How to properly write a routing table for a firewall
  - Penetration testing

Key lesson: Humility – You don't know everything (even after this course)

Books for the course

- Listed on the syllabus
  - Dan Boneh and Victor Shoup. A Graduate Course in Applied Cryptography. Online, 0.6 edition, Jan 2023.
  - Ross Anderson. *Security Engineering: A Guide for Building Dependable Systems.* Wiley, 3nd edition, 2020.
  - Matt Bishop. *Computer Security: Art and Science*. Addison-Wesley. 2003.
  - Wenliang Du. Computer & Internet Security: A Hands-on Approach. Wenliang Du, 3rd ed. edition, May 2022.
- Anderson and Boneh, et al. are available freely online (legally)

Topics for today

- Introduction
- What is computer security?
  - Definitions
- Beginners Cryptography
- One time pads
- Computational Security

- Sources: Anderson 1, SE 5

Information Security means

Ensuring software we use doesn't have flaws

Making sure the protocols we use for communication keep things secret

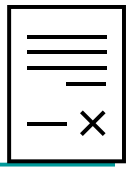
Keeping hackers and active attackers out of our systems

Keeping passive attackers from discovering business or trade secrets

Keeping accurate business records or electronic transactions

Producing enforceable contracts and agreements electronically

Example: Work Contract



What is a work contract?

- A physical document with printed information, order and cost
- Signed by both sides to show agreement

Repudiation? Dispute?

- Show the physical contract

Attacks?

- Change the text or amount
- Forge signature

What about an electronic contract?

- How do you verify it?
- How do you sign it?
- How would you resolve repudiation?

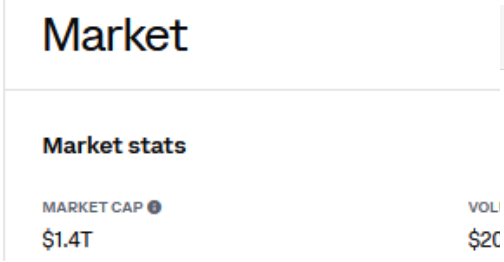
E-Commerce vs Paper Commerce

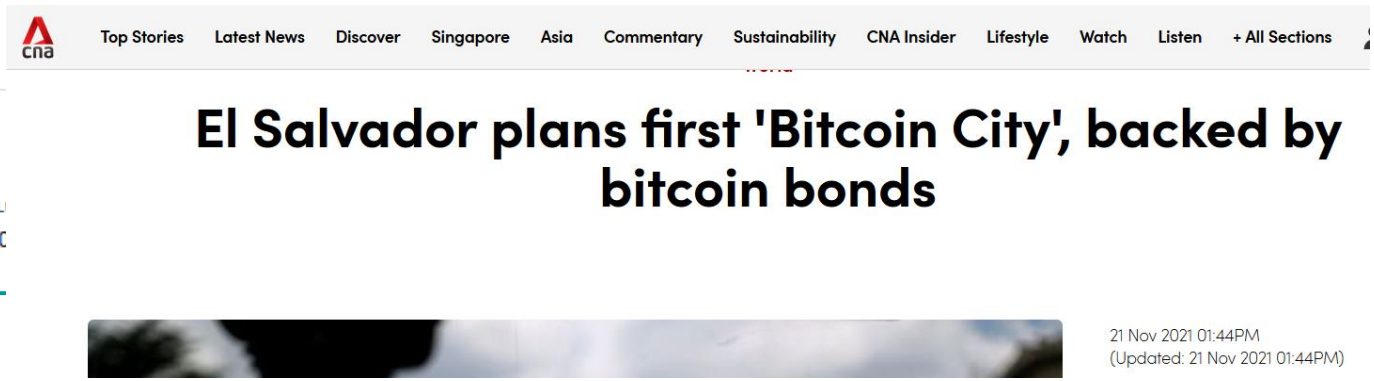
- Negotiable (סָחִיר) documents are especially difficult and hard to understand
- Can you explain these to a 6 year old? To a 60 year old?

bitcoin

ETHEREUM

Crypto? (source: coinbase)





Crypto is real?

yahoo!finance

Bitcoin is a pyramid scheme, economist says

Nick Rose · Producer

January 1, 2020

Source: The New Yorker

Table 2. The distribution of the accumulated incoming BTC's per owner

Larger or equal to	Smaller than	Number of owners
0	1	893,763
1	10	389,302
10	100	881,273
100	1,000	255,826
1,000	10,000	36,713
10,000	50,000	3,593
50,000	100,000	181
100,000	200,000	55
200,000	400,000	30
400,000	800,000	76
800,000		4

Ron, Dorit, and Adi Shamir. "Quantitative analysis of the full bitcoin transaction graph." *International Conference on Financial Cryptography and Data Security*. Springer, Berlin, Heidelberg, 2013.

The US seems to think so now

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered:

It’s complicated, though

The WHITE HOUSE

Government BTC deposited into the Strategic Bitcoin Reserve shall not be sold and shall be maintained as reserve assets of the United States utilized to meet governmental objectives in accordance with applicable law.

(b) The Secretary of the Treasury shall establish an office to administer and maintain control of custodial accounts collectively known as the “United States Digital Asset Stockpile,” capitalized with all digital assets owned by the Department of the Treasury, other than BTC, that were finally forfeited as part of criminal or civil asset forfeiture proceedings and that are not needed to satisfy requirements under 31 U.S.C. 9705 or released pursuant to subsection (d) of this section (Stockpile Assets). Within 30 days of the date of this order, each agency shall review its authorities to transfer any Stockpile Assets held by it to the United States Digital Asset Stockpile and shall submit a report reflecting the result of that review to the Secretary of the Treasury. The Secretary of the Treasury shall determine strategies for responsible stewardship of the United States Digital Asset Stockpile in accordance with applicable law.

So Far

- Introduction
- What is computer security?
  - Definitions
- Beginners Cryptography and History
- One time pads
- Computational Security
- Indistinguishability

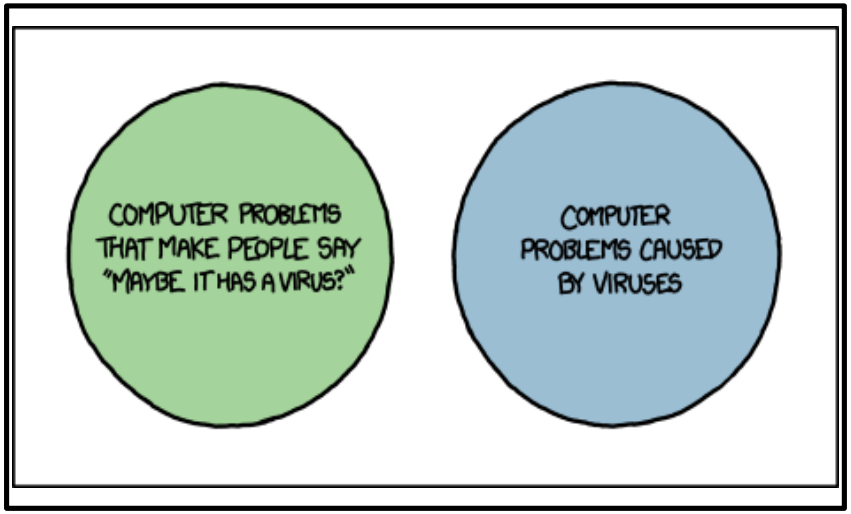
What is Computer Security?

What does security mean for a computer?

What are we worried about?

What <u>should</u> <u>we</u> be worried about?

Image source: https://imgs.xkcd.com/comics/virus_venn_diagram.png



Security Atoms

Authentication	Who are you talking to?
Transaction Integrity and Accountability	Avoid repudiation
Fault Tolerance	Know about failures Recover gracefully
Message Secrecy	Hide what you are saying
Covertness	Hide that you are even communicating

Definitions

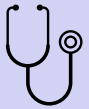
Subject

- Physical person

Principal

- Entity that participates in a security system

Role



- Set of functions assumed by people in succession

Group

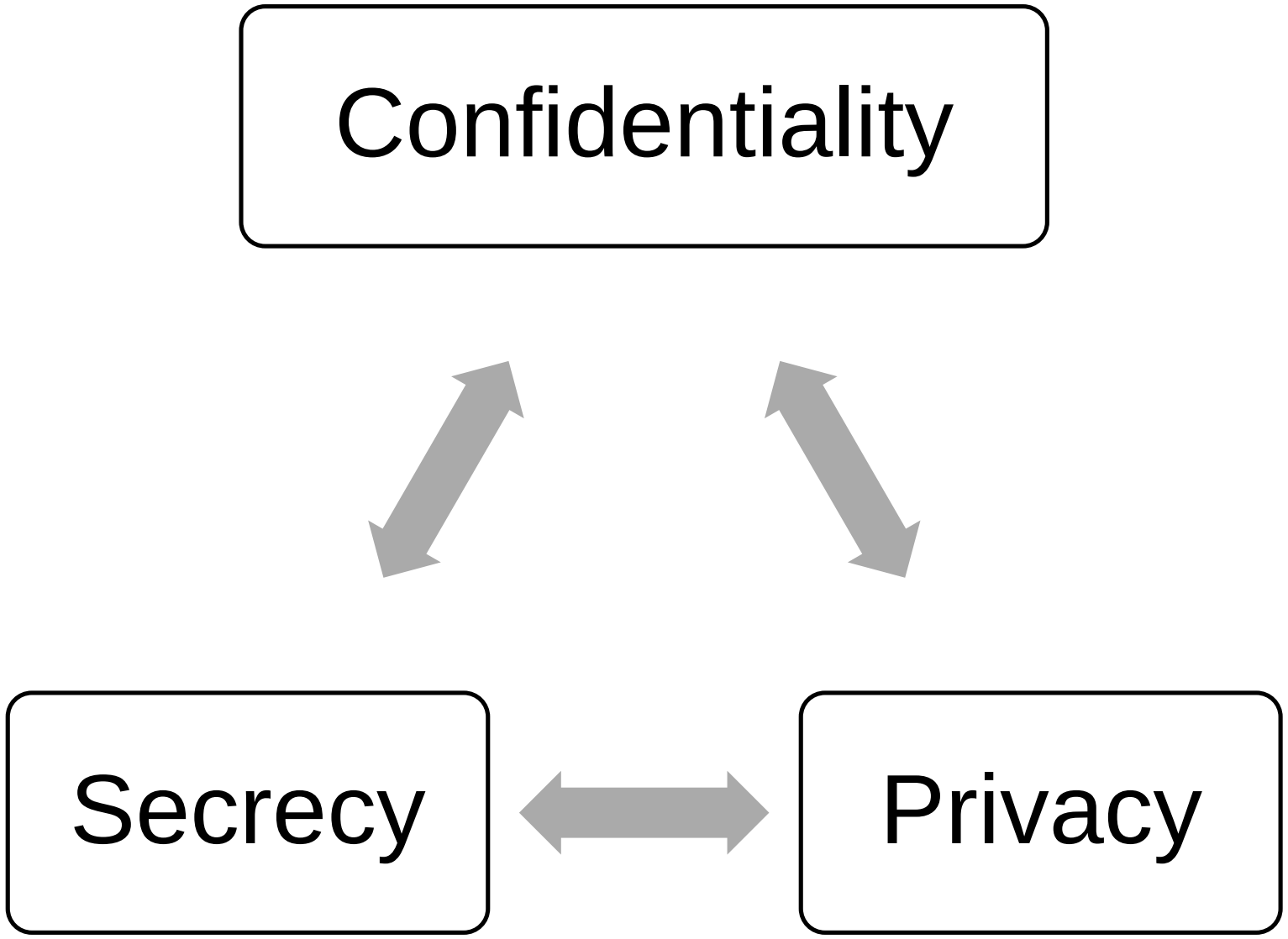
- A set of principals

Trusted

- System or component whose failure can break the security policy

Trustworthy

- A system or component that won't fail


Confidentiality
Secrecy
Privacy

Secrecy

Photo by Annie Spratt on Unsplash

Confidentiality

Photo by Ali Yahya on Unsplash

Confidentiality

Privacy

Photo by Tessa Wilson on Unsplash

Covertness

Photo by Jacek Dylag on Unsplash

Why covertness?

Phoebe Cross

Oct 4, 2019 · 4 min read

Using Tor in China

How China Is Blocking Tor

Philipp Winter and Stefan Lindskog

Karlstad University
{philwint,steflind}@kau.se

Abstract. Not only the free web is victim to China's excessive censorship, but also the Tor anonymity network: the Great Firewall of China prevents thousands of potential Tor users from accessing the network. In this paper, we investigate how the blocking mechanism is implemented, ...

Top-10 countries by possible censorship events | Top-10 countries by bridge users

Country	Mean daily users
Russia	31403 (44.30 %)
United States	6955 (9.81 %)
Germany	3307 (4.66 %)
Iran	2854 (4.03 %)
Netherlands	1736 (2.45 %)
United Kingdom	1733 (2.44 %)
France	1697 (2.39 %)
China	1438 (2.03 %)
Belarus	1394 (1.97 %)
India	1323 (1.87 %)

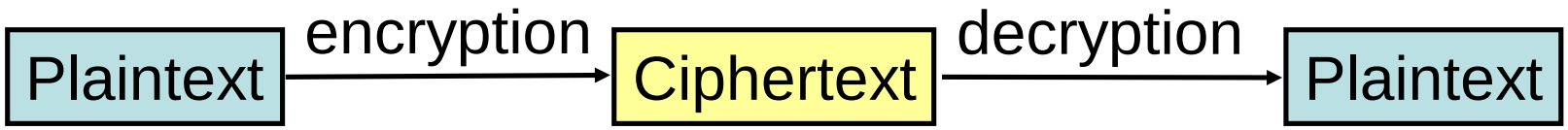
So Far

- Introduction
- What is computer security?
  - Definitions
- Beginners Cryptography
- One time pads
- Computational Security
- Indistinguishability

Κρυπτογραφία (Cryptography)

- Traditionally, most computer security courses start with an introduction to Cryptography
  - From the Greek "kryptos" and "graphia" for “secret writing”
- Secrecy: Prevent others from understanding a message
- Integrity: Detect if a message/file was changed since sent/stored
- Authentication: Verify the identity of the source of a message
- Non-repudiation: Inability to deny a true event or message

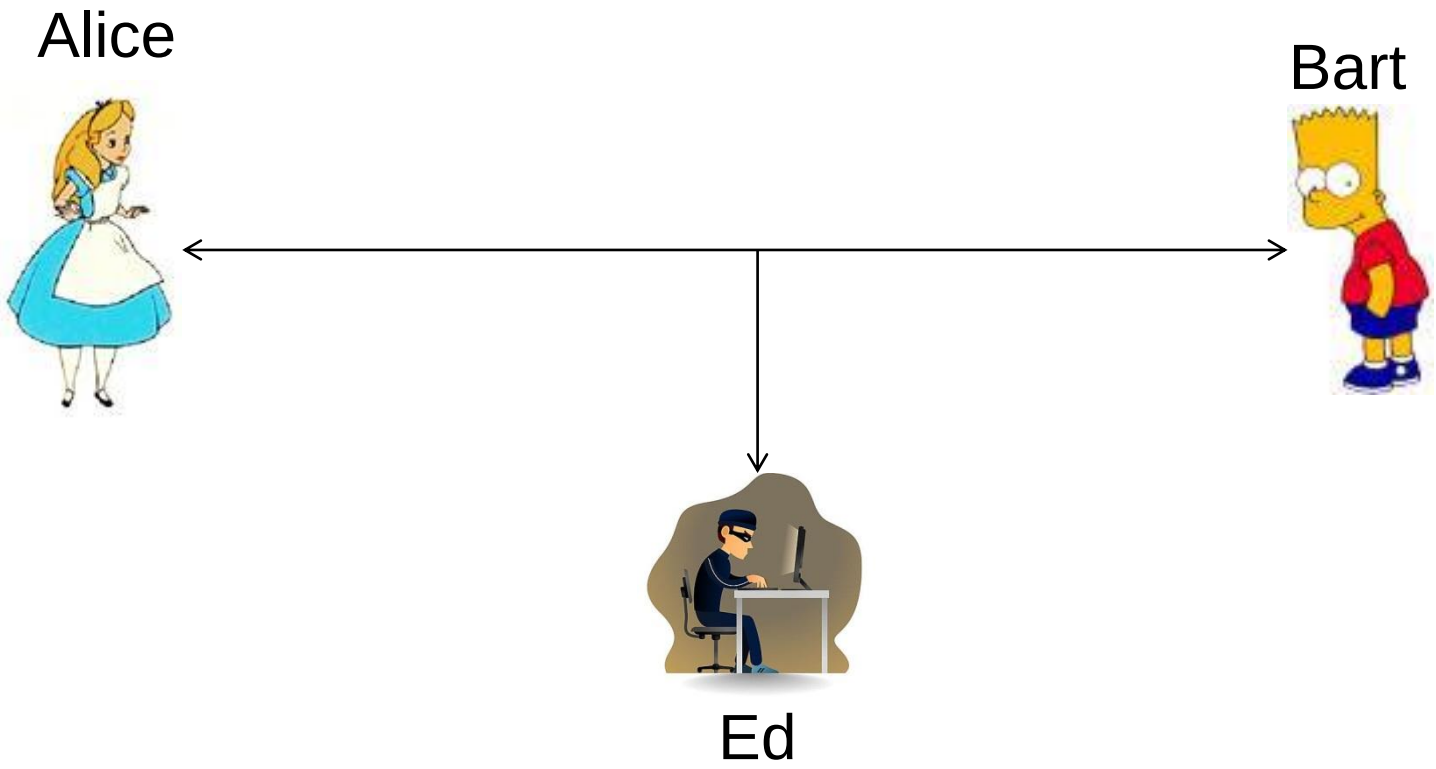
Terminology



- Cryptographer
  - Invents cryptosystems
- Cryptanalyst
  - Breaks cryptosystems
- Cryptology
  - Study of crypto systems
- Cipher
  - Mechanical way of encrypting text or data
- Code
  - Semantic translation: “eat breakfast tomorrow” = “attack on Thursday” (or use Navajo!)

A First Cipher

Games



Kinds of Cryptographic Analysis

Ciphertext Only Attacks

Given:

1. Ciphertext
2. Algorithm (maybe)

Goals:

1. Find (correct) plain text
2. Find key info
3. Find algorithm (if not given)

May not need all goals

Known Plaintext Attacks

Given:

1. Full or partial plaintext
2. Ciphertext
3. Algorithm (maybe)

Goals:

1. Find key info
2. Find algorithm (if not given)

Kinds of Cryptographic Analysis

Chosen Plaintext Attacks

Given:

1. Full Plaintext (chosen by attacker)
2. Ciphertext
3. Algorithm (maybe)

Goals:

1. Find key info
2. Find algorithm (if not given)

So Far

- Introduction
- What is computer security?
  - Definitions
- Beginners Cryptography
- One time pads
- Computational Security
- Indistinguishability

Perfect Substitution Ciphers

$$\begin{array}{rccccc} & p_1 & p_2 & p_3 & \dots & p_n \\ \oplus & b_1 & b_2 & b_3 & \dots & b_n \\ \hline & c_1 & c_2 & c_3 & \dots & c_n \end{array}$$

Choose a string of random bits the same length as the plaintext, XOR them to obtain the ciphertext.

Perfect Secrecy

- Probability that a given message is encoded in the ciphertext is unaltered by knowledge of the ciphertext

Why is it Perfect?

$$\begin{array}{rccccc} & p_1 & p_2 & p_3 & \dots & p_n \\ \oplus & b_1 & b_2 & b_3 & \dots & b_n \\ \hline & c_1 & c_2 & c_3 & \dots & c_n \end{array}$$

Proof:

Given any plaintext message and any ciphertext. I can construct a key that will produce the ciphertext from the plaintext.

Why is it perfect?

Alice: I can prove to you THIS is the original message
Bob: I can prove to you THAT is the original message
Claire: I can prove to you JUMP is the original message

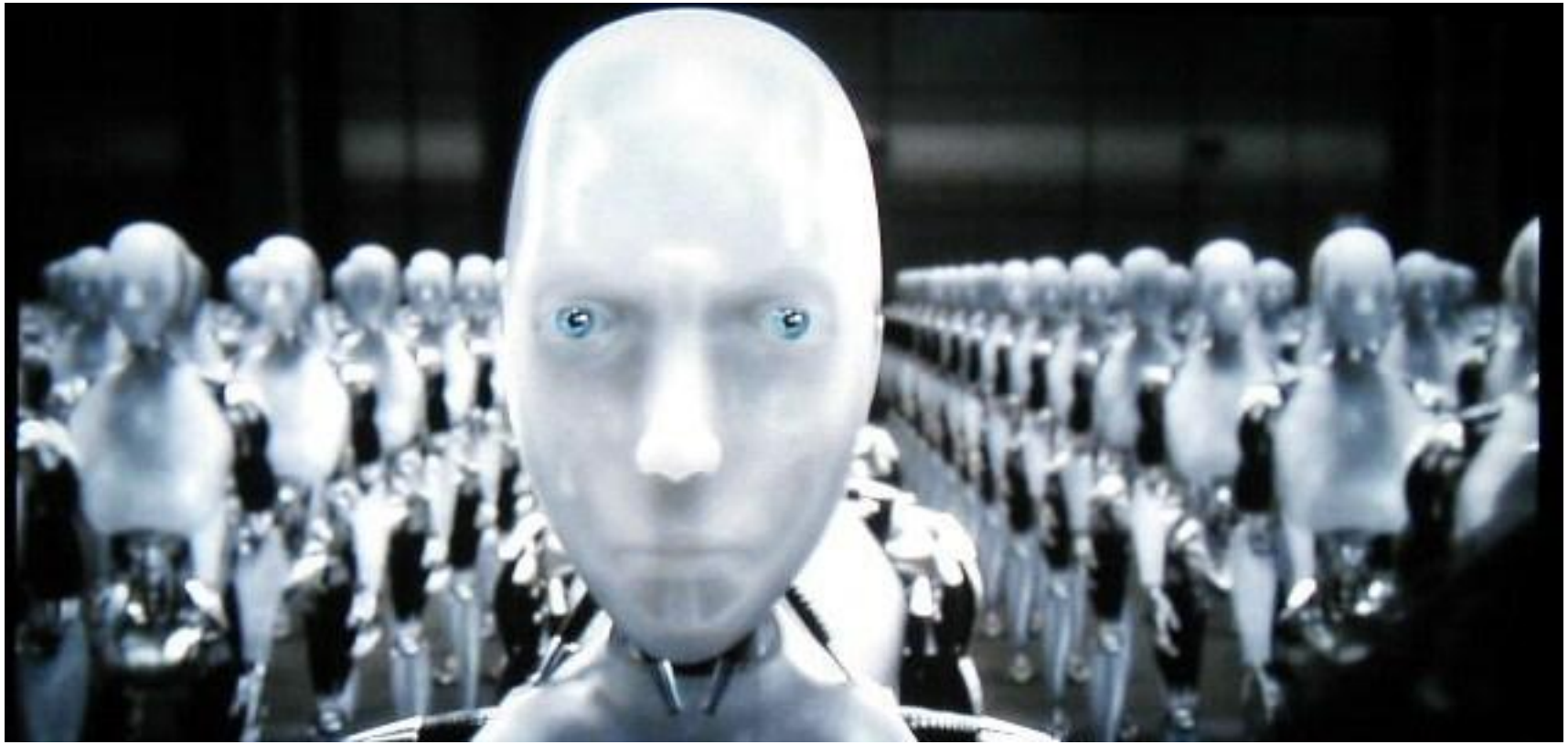


Image source: https://truedemocracyparty.net/wp-content/uploads/IROBOT2.jpg

Ciphertext = jktp

Key	Result	Key	Result	Key	Result
aaaa	jktp	duhn	meac	tevv	cook
aaab	jktq	duho	mead	tevw	cool
aaac	jktr	duhp	meae	tevx	coom
aaad	jkts	duhq	meaf	tevy	coon
aaae	jktt	duhr	meag	tevz	cooo
aaaf	jktu	duhs	meah	tewd	cops
aaag	jktv	duht	meai	tewe	copt
aaah	jktw	duhu	meaj	tewf	copu
aaai	jktx	duhv	meak	tewg	copv
aaaj	jkty	duhw	meal	tewh	copw
aaak	jktz	duhx	meam	tewi	copx
aaal	jkta	duhy	mean	tewj	copy
…	….				

Potential results: 26^4=456,976

File size: 5.22MB

Full file 

Key point: All 4 letter words are potential solutions

One-time Pads

Another name for Perfect Substitution

Really used by US agents in Russia

- Physical pad of paper
- List of random numbers
- Pages were torn out and destroyed after use
- “Numbers Stations”?

Vernam Cipher

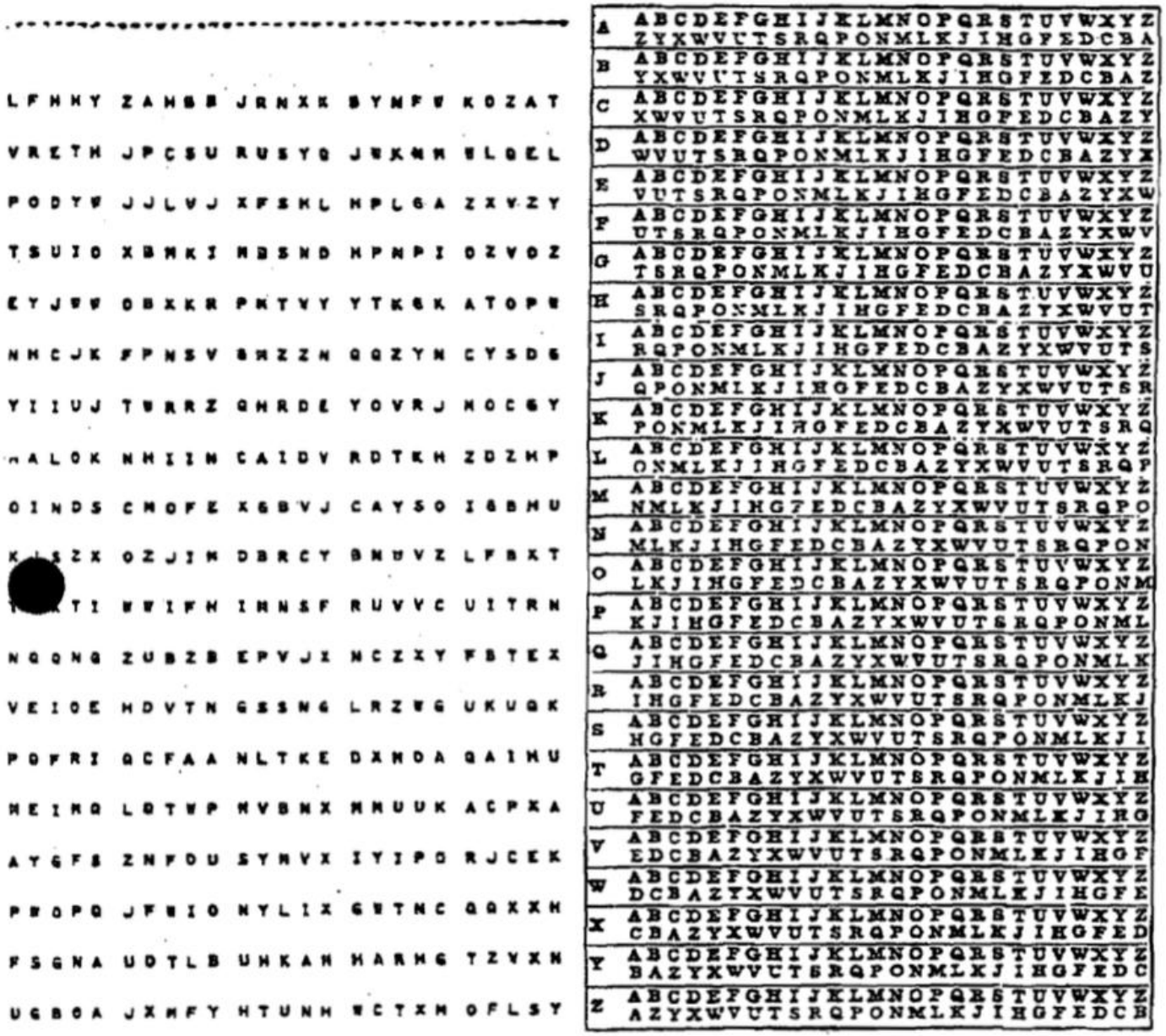
- Used by AT&T
- Random sequence stored on punch tape

Not practical for computer security…

Leo Marks (UK): Reinvented OTP in WWII

Image credits: http://www.mishalov.com/Marks.html

NSA – One time pad



A	ABCDEFGHIJKLMNOPQRSTUVWXYZ ZYXWVUTSRQPONMLKJIHGFEDCBA
B	ABCDEFGHIJKLMNOPQRSTUVWXYZ YXWVUTSRQPONMLKJIHGFEDCBAZ
C	ABCDEFGHIJKLMNOPQRSTUVWXYZ XWVUTSRQPONMLKJIHGFEDCBAZY
D	ABCDEFGHIJKLMNOPQRSTUVWXYZ WVUTSRQPONMLKJIHGFEDCBAZYX
E	ABCDEFGHIJKLMNOPQRSTUVWXYZ VUTSRQPONMLKJIHGFEDCBAZYXW
F	ABCDEFGHIJKLMNOPQRSTUVWXYZ UTSRQPONMLKJIHGFEDCBAZYXWV
G	ABCDEFGHIJKLMNOPQRSTUVWXYZ TSRQPONMLKJIHGFEDCBAZYXWVU
H	ABCDEFGHIJKLMNOPQRSTUVWXYZ SRQPONMLKJIHGFEDCBAZYXWVUT
I	ABCDEFGHIJKLMNOPQRSTUVWXYZ RQPONMLKJIHGFEDCBAZYXWVUTS
J	ABCDEFGHIJKLMNOPQRSTUVWXYZ QPONMLKJIHGFEDCBAZYXWVUTSR
K	ABCDEFGHIJKLMNOPQRSTUVWXYZ PONMLKJIHGFEDCBAZYXWVUTSRQ
L	ABCDEFGHIJKLMNOPQRSTUVWXYZ ONMLKJIHGFEDCBAZYXWVUTSRQP
M	ABCDEFGHIJKLMNOPQRSTUVWXYZ NMLKJIHGFEDCBAZYXWVUTSRQPO
N	ABCDEFGHIJKLMNOPQRSTUVWXYZ MLKJIHGFEDCBAZYXWVUTSRQPON
O	ABCDEFGHIJKLMNOPQRSTUVWXYZ LKJIHGFEDCBAZYXWVUTSRQPONM
P	ABCDEFGHIJKLMNOPQRSTUVWXYZ KJIHGFEDCBAZYXWVUTSRQPONML
Q	ABCDEFGHIJKLMNOPQRSTUVWXYZ JIHGFEDCBAZYXWVUTSRQPONMLK
R	ABCDEFGHIJKLMNOPQRSTUVWXYZ IHGFEDCBAZYXWVUTSRQPONMLKJ
S	ABCDEFGHIJKLMNOPQRSTUVWXYZ HGFEDCBAZYXWVUTSRQPONMLKJI
T	ABCDEFGHIJKLMNOPQRSTUVWXYZ GFEDCBAZYXWVUTSRQPONMLKJIH
U	ABCDEFGHIJKLMNOPQRSTUVWXYZ FEDCBAZYXWVUTSRQPONMLKJIHG
V	ABCDEFGHIJKLMNOPQRSTUVWXYZ EDCBAZYXWVUTSRQPONMLKJIHGF
W	ABCDEFGHIJKLMNOPQRSTUVWXYZ DCBAZYXWVUTSRQPONMLKJIHGFE
X	ABCDEFGHIJKLMNOPQRSTUVWXYZ CBAZYXWVUTSRQPONMLKJIHGFED
Y	ABCDEFGHIJKLMNOPQRSTUVWXYZ BAZYXWVUTSRQPONMLKJIHGFEDC
Z	ABCDEFGHIJKLMNOPQRSTUVWXYZ AZYXWVUTSRQPONMLKJIHGFEDCB

Image via; By US National Security Agency - http://www.governmentattic.org/18docs/Hist_US_COMSEC_Boak_NSA_1973u.pdf
A History of U.S. Communications Security; the David G. Boak Lectures, National Security Agency (NSA),
Volumes I, 1973, Volumes II 1981,
partially released 2008, additional portions declassified October 14, 2015,
Public Domain, https://commons.wikimedia.org/w/index.php?curid=45783652

Problems with “Perfect” Substitution

Key is the same length as the plaintext

- Sender and receiver must agree on the same random sequence
- Not any easier to transmit key securely than to transmit plaintext securely

Need to be able to generate many truly random bits

- Pseudorandom numbers generated by an algorithm aren’t good enough for long messages

Can’t reuse the key

- Not enough confusion

Followup: Venona [Video, Wikipedia, docs]

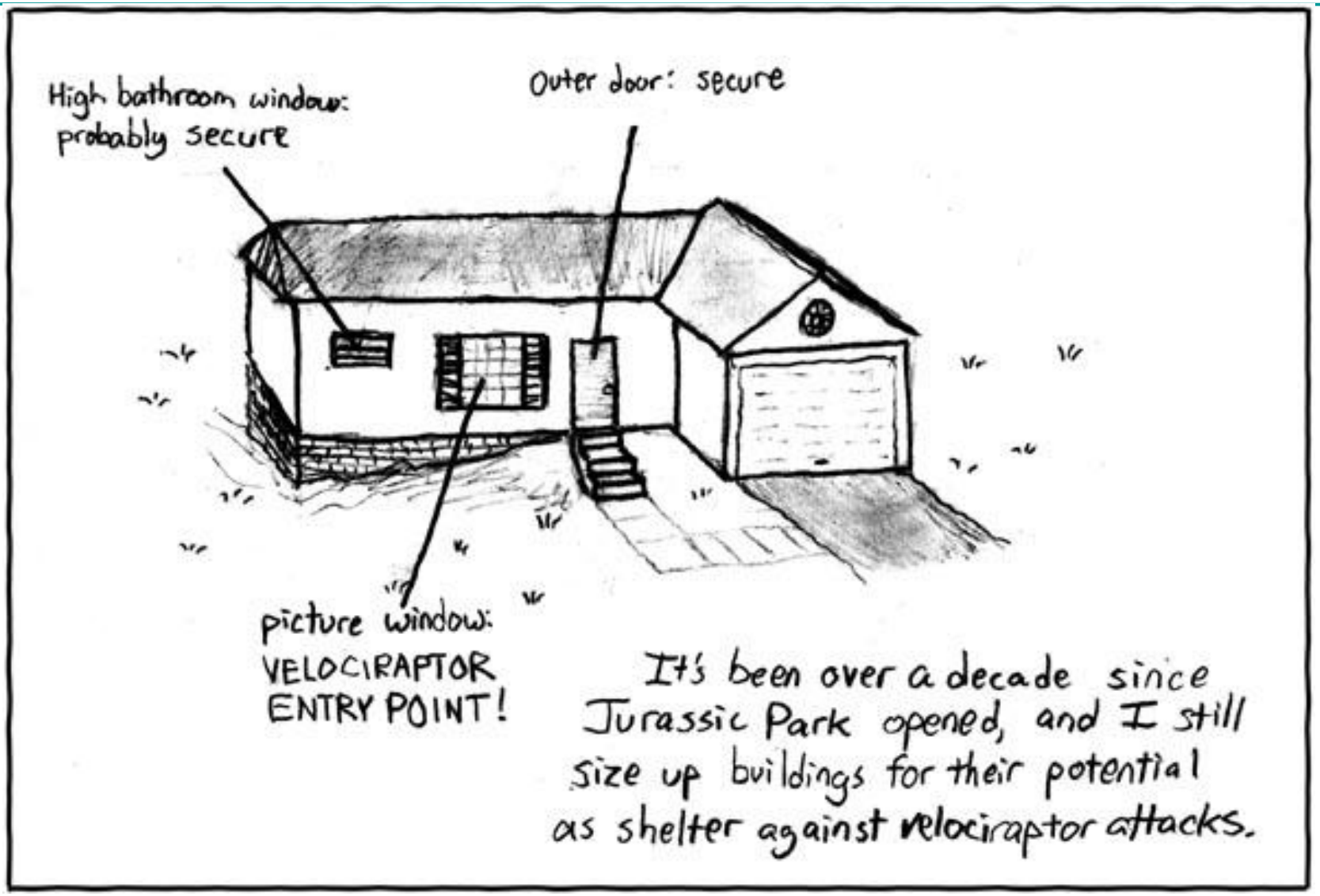
So Far

- Introduction
- What is computer security?
  - Definitions
- Beginners Cryptography
- One time pads
- Computational Security
- Indistinguishability

Computational Security

- Perfect Ciphers are *unconditionally secure*
  - No amount of computation will help crack the cipher (i.e. the *only* strategy is brute force)
- What is a *brute force attack*?
- Everything else is computationally secure

https://xkcd.com/87/



Computational Security

In practice, strive for *computationally security*

- Given enough power, attacker can crack the cipher (brute force)
- But, an attacker with *bounded resources* is extremely unlikely to crack it

Example: Assume attacker has only polynomial time, then encryption algorithm that can't be inverted in less than exponential time is secure.

Example: Encryption can be cracked in 10 years from today.

Avoid **trapdoors or shortcuts**

So Far

- Introduction
- What is computer security?
  - Definitions
- Beginners Cryptography and History
- One time pads
- Computational Security
- Indistinguishability

What's a good cipher?

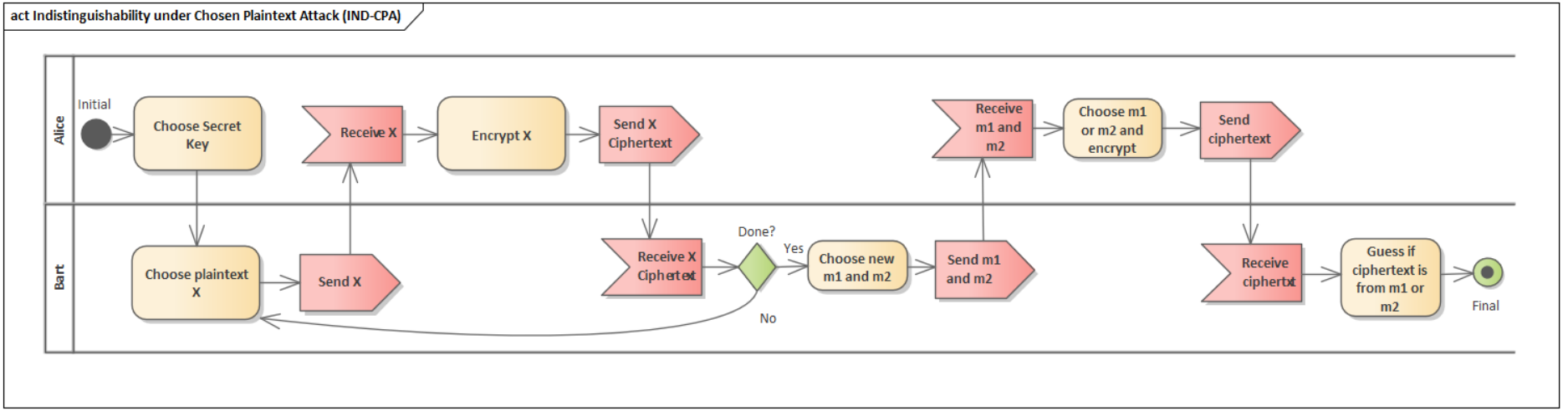
Indistinguishability under Chosen Plaintext Attack (IND-CPA)

Game:

1. Alice chooses a secret key
2. Bart sends Alice plaintexts to encrypt. Alice encrypts and returns them.
3. Bart sends Alice two (new) messages m_1 and m_2
4. Alice flips a coin and encrypts either m_1 or m_2 based on it → c_1. Alice sends Bart c_1
5. Bart must guess whether c_1 is the encryption of m_1 or m_2

Bart wins if he can guess better than 50% using a *probabilistic polynomial time Turing machine*

IND-CPA Imagined



What's a good cipher?

Indistinguishability under Chosen Ciphertext Attack (IND-CCA1)

Game:

1. Alice chooses a secret key
2. Bart sends Alice plaintexts to encrypt or decrypt. Alice encrypts or decrypts and returns them.
3. Bart sends Alice two (new) messages m_1 and m_2
4. Alice flips a coin and encrypts either m_1 or m_2 based on it → c_1. Alice sends Bart c_1
5. Bart must guess whether c_1 is the encryption of m_1 or m_2

Bart wins if he can guess better than 50% using a *probabilistic polynomial time Turing machine*

What's a good cipher?

Indistinguishability under Adaptive Chosen Ciphertext Attack (IND-CCA2)

Game:

1. Alice chooses a secret key
2. Bart sends Alice plaintexts to encrypt or decrypt. Alice encrypts or decrypts and returns them.
3. Bart sends Alice two (new) messages m_1 and m_2
4. Alice flips a coin and encrypts either m_1 or m_2 based on it → c_1. Alice sends Bart c_1
5. Bart can ask Alice to decrypt any message except for c_1
6. Bart must guess whether c_1 is the encryption of m_1 or m_2

Bart wins if he can guess better than 50% using a *probabilistic polynomial time Turing machine*

How they relate

$$\text{IND-CCA2} \Rightarrow \text{IND-CCA1} \Rightarrow \text{IND-CPA}$$

Conclusion

- Introduction
- What is computer security?
  - Definitions
- Beginners Cryptography and History
- One time pads
- Computational Security
- Indistinguishability