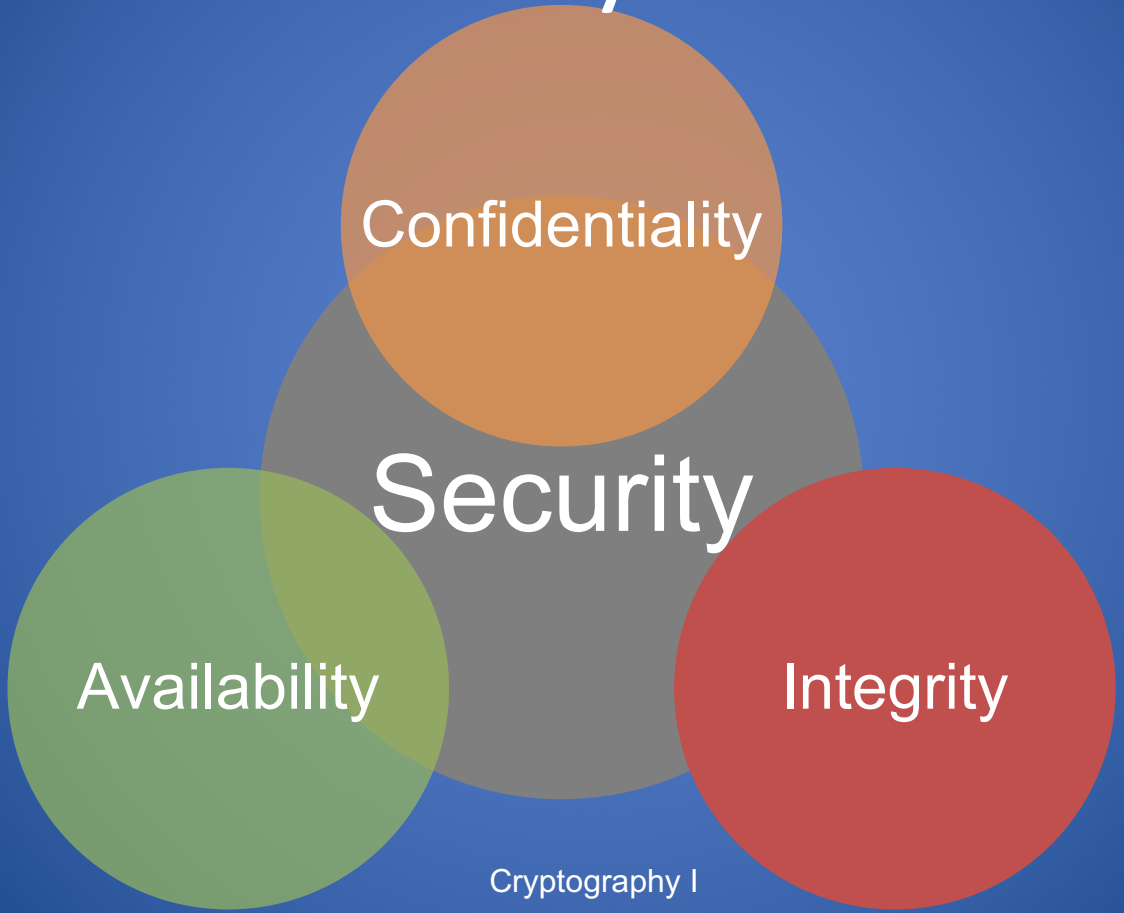
Cryptography I

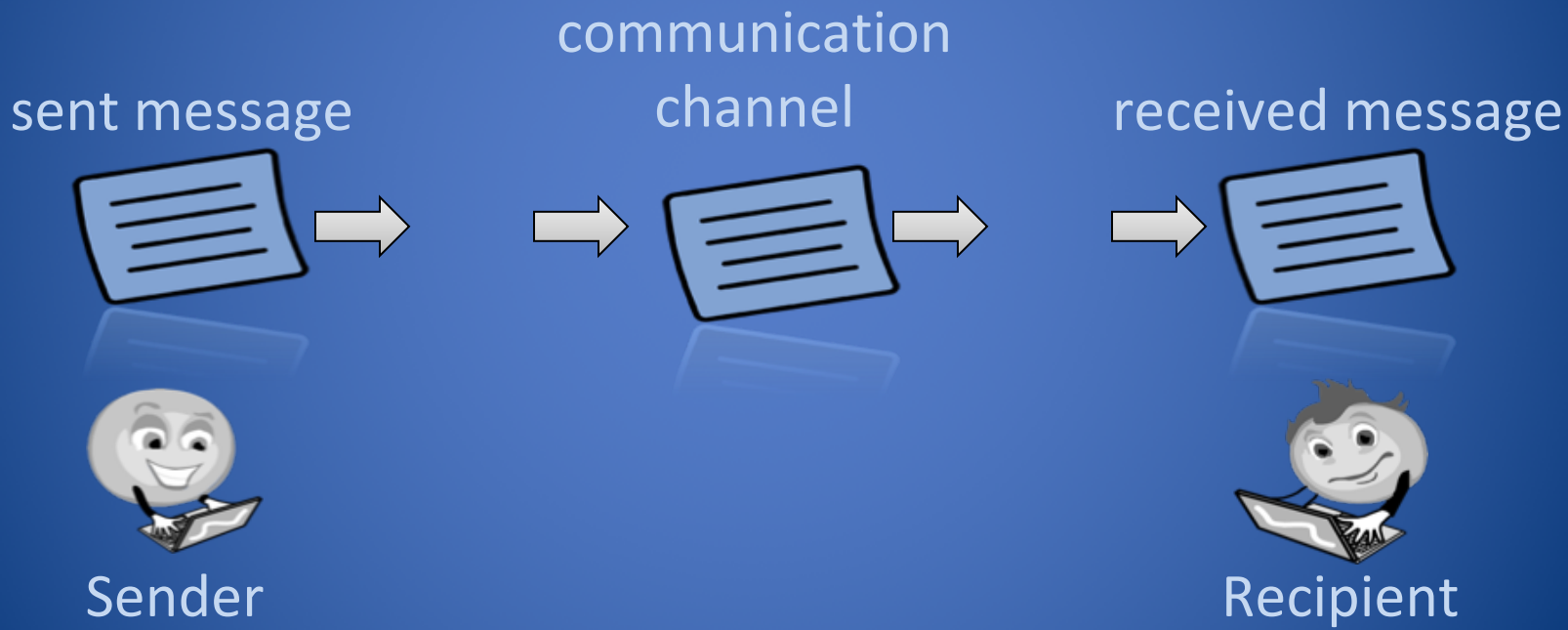
CS 166: Introduction to Computer Systems Security

Security Goals

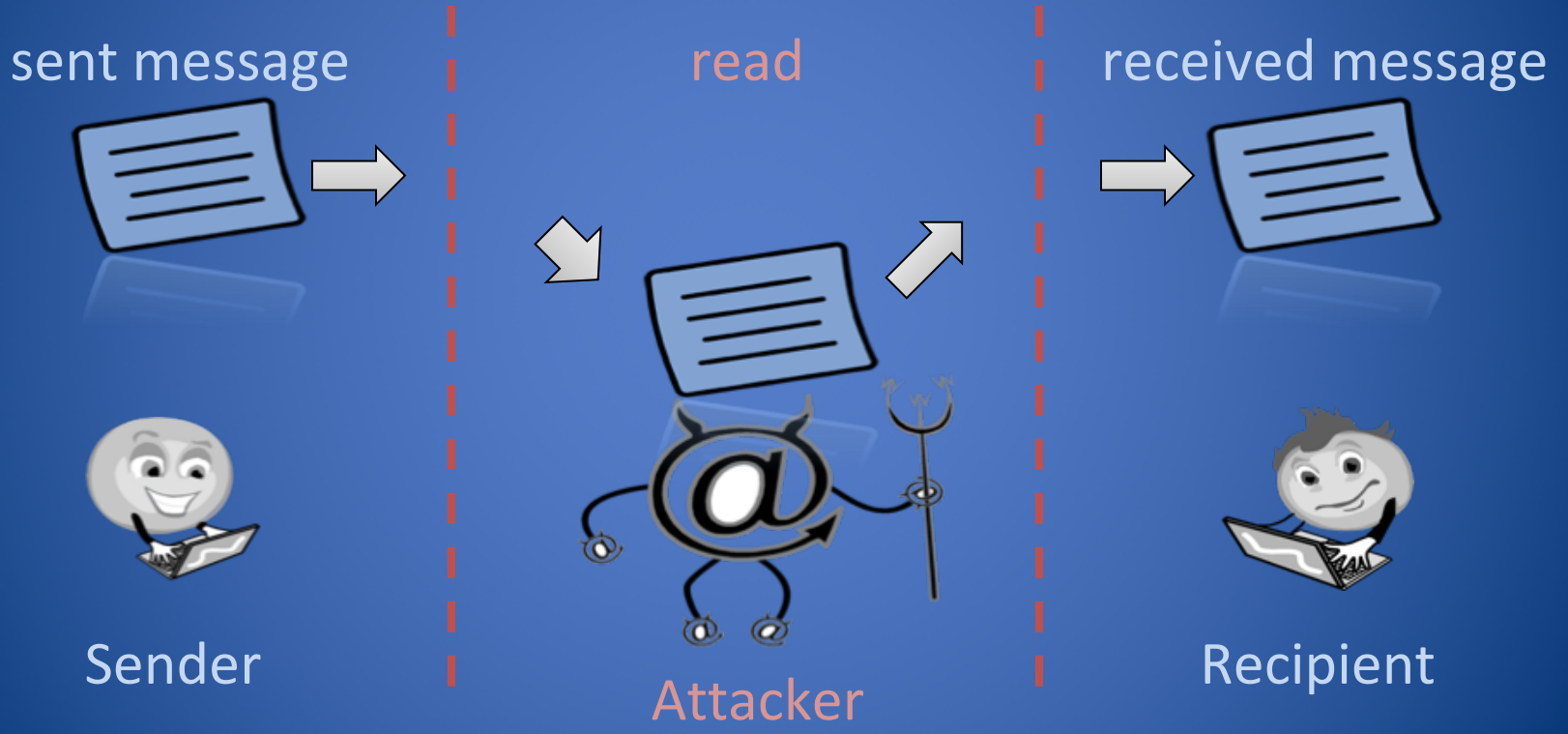


Attacks on Communication

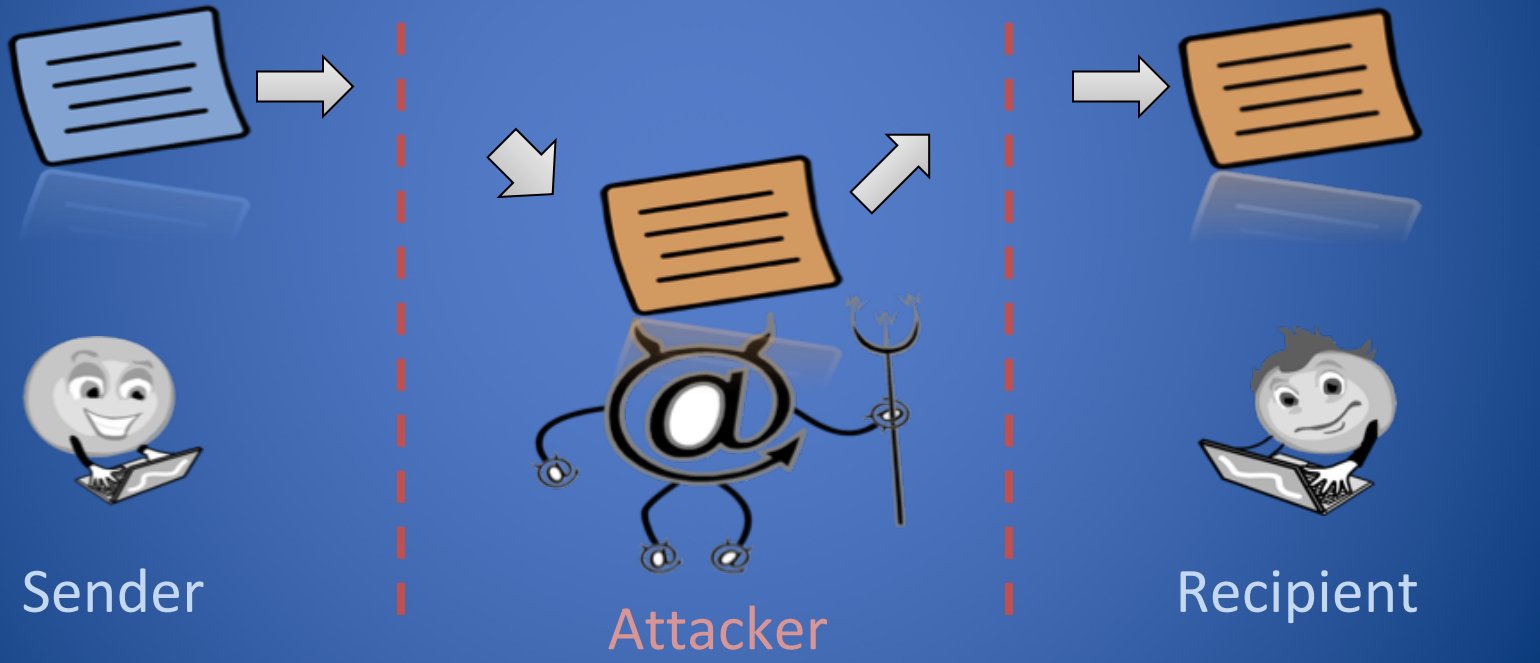
Standard Communication



Eavesdropping



Tampering

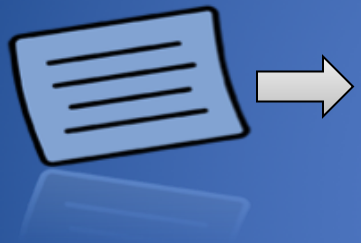

sent message
modify
received message
Sender
Attacker
Recipient

Blocking

sent message

drop

received message



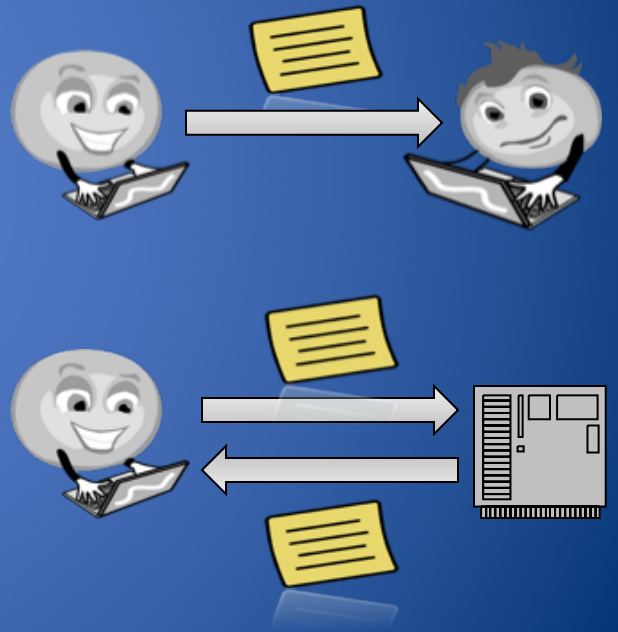
Sender

Attacker

Recipient

Cryptography

- Cryptography provides methods for assuring the confidentiality and integrity of data that is
  - transmitted over communication channels (e.g., web pages and email messages)
  - stored on devices (e.g., files on a laptop or data center)

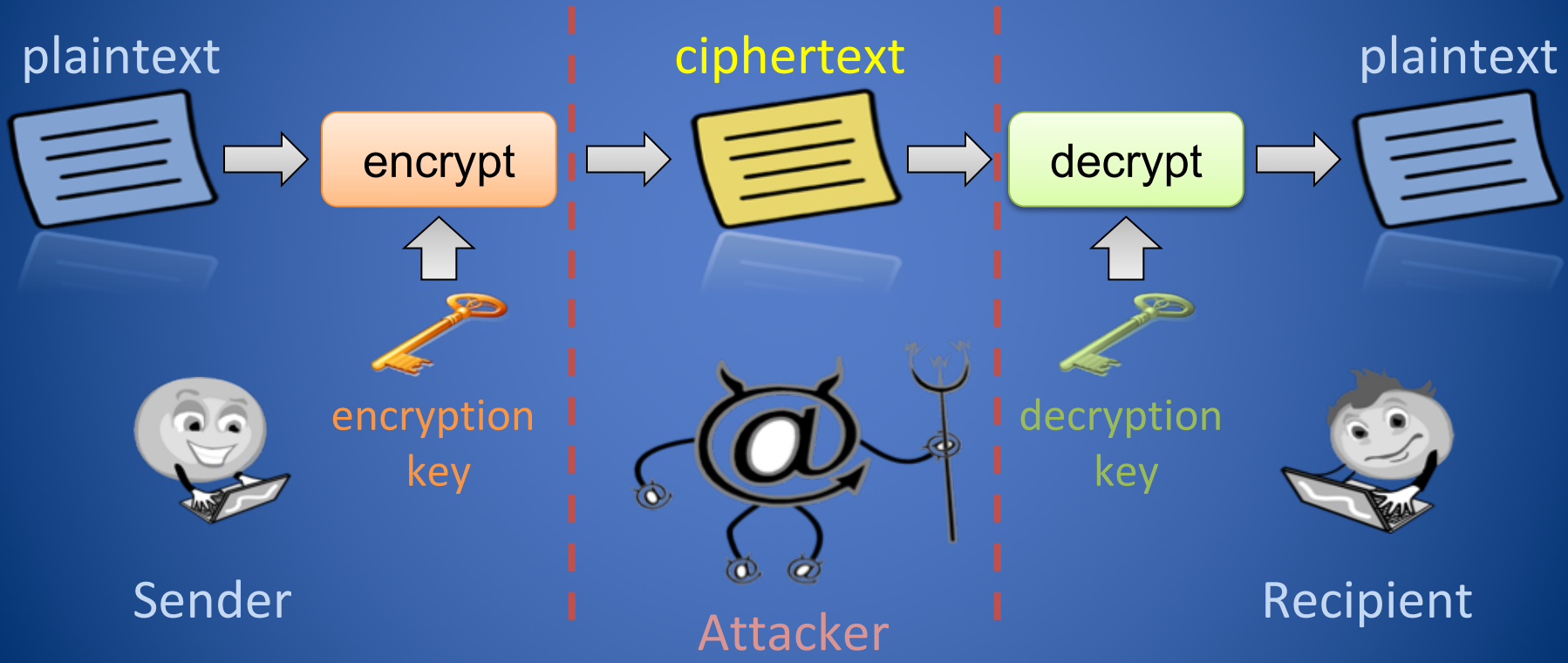


Open Design Principle

- Publicly available system architecture and algorithms
- Security relies solely on keeping keys secret
- Formulated by Auguste Kerckhoffs in 1883
- Opposite of “security by obscurity”

Image source: https://en.wikipedia.org/wiki/Auguste_Kerckhoffs#/media/File:Auguste_Kerckhoffs.jpg

Encrypted Communication



Encryption

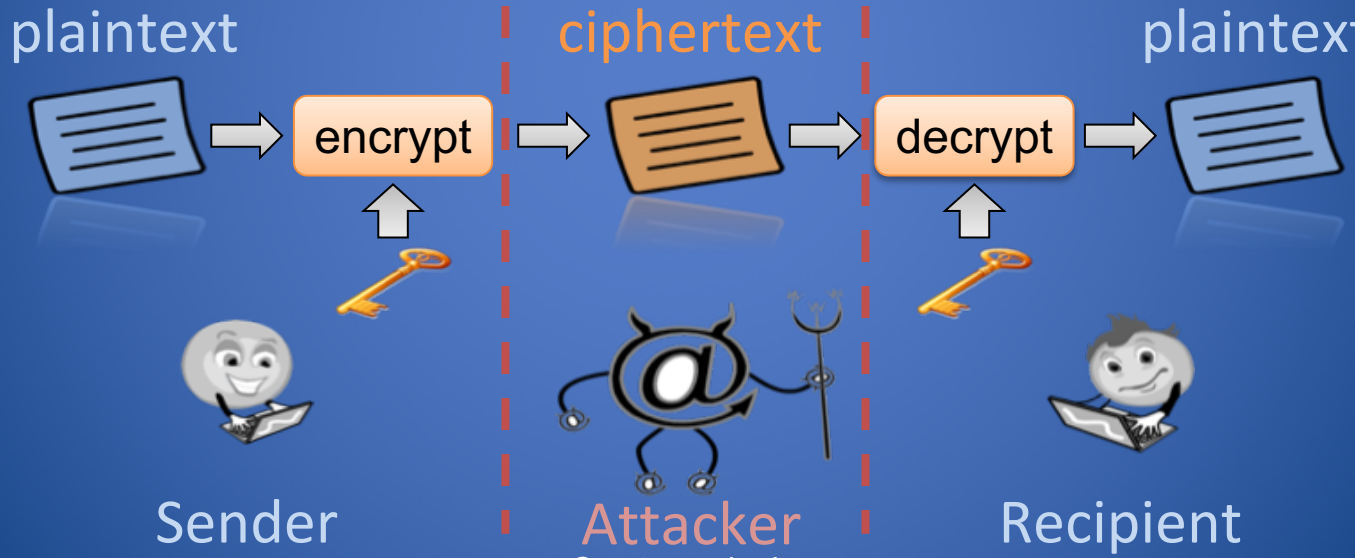
- Encryption allows to secure communication
  - Originally focused on confidentiality alone
- The encryption algorithm combines the plaintext with the encryption key to produce the ciphertext

  - The ciphertext is transmitted instead of the plaintext
- The decryption algorithm combines the ciphertext with the decryption key to return the plaintext

  - Only the intended recipient should have the secret key
- Encryption and decryption should be computationally infeasible without the corresponding keys

Symmetric Encryption

- Same key used for encryption and decryption
- Encryption and decryption algorithms are one the reverse of the other



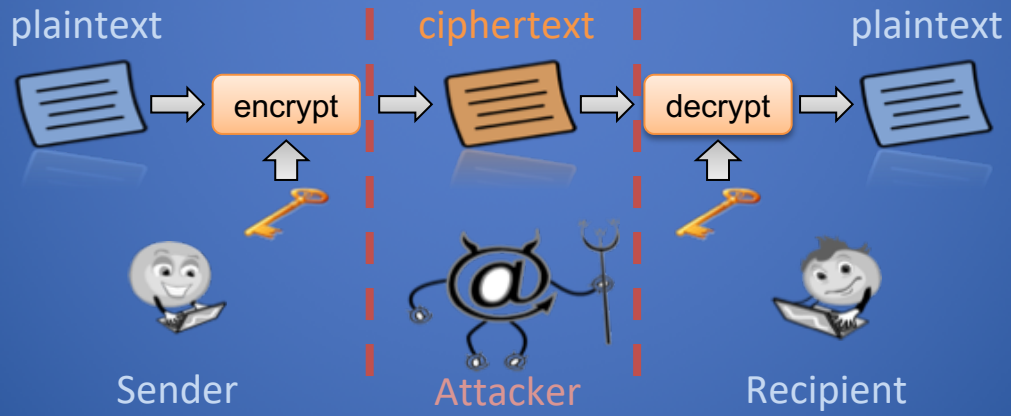
Symmetric Encryption

Advantage:

- Conceptual simplicity

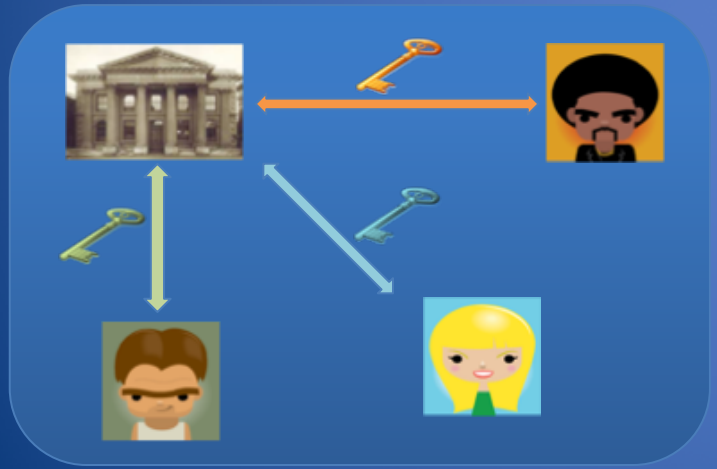
Disadvantage:

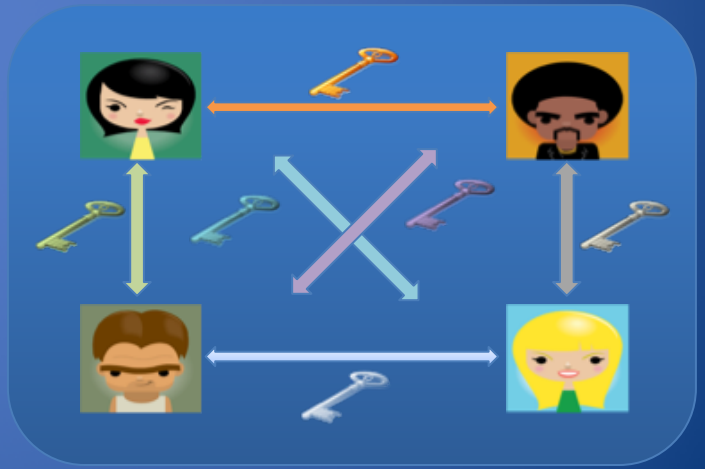
- Secure channel to set up key



Symmetric Key Distribution

- A distinct keys needs to be set up for each pair of communicating users
- Quadratic number of keys for pairwise communication





Classic Symmetric Encryption

Julius Caesar's Cipher

- Encryption
  - replace A with D
  - replace B with E
  - replace C with F
  - …
  - replace X with A
  - replace Y with B
  - replace Z with C
- Encryption key
  - Forward alphabet shift: +3
- Decryption key
  - Reverse alphabet shift: –3

AVE → DZH

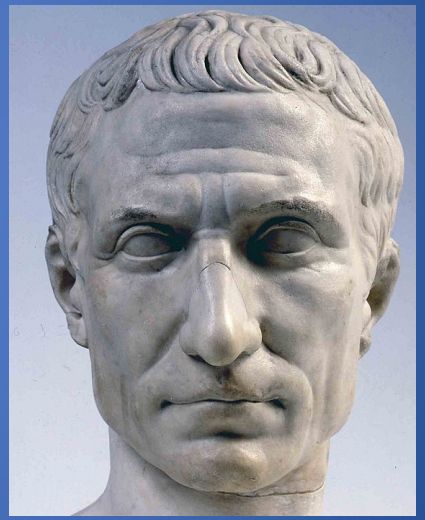


Image source:
https://en.wikipedia.org/wiki/Julius_Caesar#/media/File:Gaius_Iulius_Caesar_(Vatican_Museum).jpg

Alphabet Shift Cipher

- Generalization of Caesar's cipher
- Replace each character c of the plaintext with the character k positions after c in the alphabet
- Key for encryption and decryption: number k
- Insecure encryption method
- Can be easily cracked by trying all possible values of k between 1 and the size of the alphabet

Substitution Cipher

- Arbitrary permutation of the characters
  - A → K
  - B → T
  - C → G
  - …

CAB → GKT

- Key: permutation of the alphabet characters (e.g., KTG …)
- Number of possible keys for a 26-character alphabet ≈ 4×10^{26}
- Unfeasible to try all possible keys but …
- Can be cracked by frequency analysis
  - most frequent letters in English: e, t, o, a, n, i, ...
  - most frequent digrams: th, in, er, re, an, ...
  - most frequent trigrams: the, ing, and, ion, ...
- Attack first described in a 9th century book by al-Kindi

Frequency Analysis

PCQ VMJYPD LBYK LYSO KBXBJXWXV BXV ZCJPO EYPD KBXBJYUXJ LBJOO KCPK. CP LBO LBCMKXPV XPV IYJKL PYDBL, QBOP KBO BXV OPVOV LBO LXRO CI SX'XJMI, KBO JCKO XPV EYKKOV LBO DJCMPV ZOICJO BYS, KXUYPD: “DJOXL EYPD, ICJ X LBCMKXPV XPV CPO PYDBLK Y BXNO ZOOP JOACMPLYPD LC UCM LBO IXZROK CI FXKL XDOK XPV LBO RODOPVK CI XPAYOPL EYPDK. SXU Y SXEO KC ZCRV XK LC AJXNO X IXNCMJ CI UCMJ SXGOKLU?”

OFYRCDMO, LXROK IJCS LBO LBCMKXPV XPV CPO PYDBLK

Example from

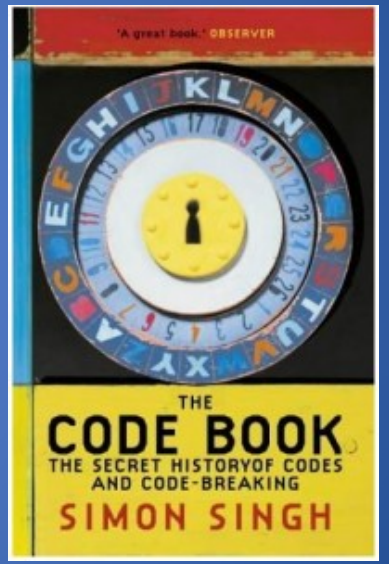


Image source: https://simonsingh.net

Frequency Analysis (cont.)

PCQ VMJYPD THYK TYSE KHXHJXWXV HXV ZCJPE EYPD KHXHJYUXJ THJEE KCPK. CP THE THCMKXPV XPV IYJKT PYDHT, QHEP KHO HXV EPVEV THE LXRE CI SX'XJMI, KHE JCKE XPV EYKKEV THE DJCMPV ZEICJE HYS, KXUYPD: "DJEXT EYPD, ICJ X THCMKXPV XPV CPE PYDHTK Y HXNE ZEEP JEACMPTYPD TC UCM THE IXZREK CI FXKT XDEK XPV THE REDEPVK CI XPAYEPT EYPDK. SXU Y SXEE KC ZCRV XK TC AJXNE X IXNCMJ CI UCMJ SXGEKTU?"

EFYRCDME, TXREK IJCS THE THCMKXPV XPV CPE PYDBTK

L → T

B → H

O → E

More guesses

J → R

K → S

X → A

Frequency Analysis (cont.)

PCQ VMRYPD THYS TYSE SHAHRAWAV HAV ZCRPE EYPD SHAHRYUAR THREE SCPS. CP THE THCMSAPV APV IYRST PYDHT, QHEP SHO HAV EPVEV THE LARE CI SA'ARMI, SHE RCSE APV EYSSEV THE DRCMPV ZEICRE HYS, SAUYPD: "DREAT EYPD, ICR A THCMSAPV APV CPE PYDHTS Y HANE ZEEP REACMPTYPD TC UCM THE IAZRES CI FAST ADES APV THE REDEPVS CI APAYEPT EYPDS. SAU Y SAEE SC ZCRV AS TC ARANE A IANCMR CI UCMR SAGESTU?"

EFYRCDME, TARES IRCS THE THCMSAPV APV CPE PYDBTS

L → T

B → H

O → E

J → R

K → S

X → A

Decryption

PCQ VMJYPD LBYK LYSO KBXBJXWXV BXV ZCJPO EYPD KBXBJYUXJ LBJOO KCPK. CP LBO LBCMKXPV XPV IYJKL PYDBL, QBOP KBO BXV OPVOV LBO LXRO CI SX'XJMI, KBO JCKO XPV EYKKOV LBO DJCMPV ZOICJO BYS, KXUYPD: “DJOXL EYPD, ICJ X LBCMKXPV XPV CPO PYDBLK Y BXNO ZOOP JOACMPLYPD LC UCM LBO IXZROK CI FXKL XDOK XPV LBO RODOPVK CI XPAYOPL EYPDK. SXU Y SXEO KC ZCRV XK LC AJXNO X IXNCMJ CI UCMJ SXGOKLU?”

OFYRCDMO, LXROK IJCS LBO LBCMKXPV XPV CPO PYDBLK

Now during this time Shahrazad had borne king Shahriyar three sons. On the thousand and first night, when she had ended the tale of Ma'aruf, she rose and kissed the ground before him, saying: “great king, for a thousand and one nights I have been recounting to you the fables of past ages and the legends of ancient kings. May I make so bold as to crave a favour of your majesty?”

Epilogue, Tales from the Thousand and One Nights

One-Time Pad

Bitwise XOR

X	Y	X $\oplus$ Y
0	0	0
0	1	1
1	0	1
1	1	0

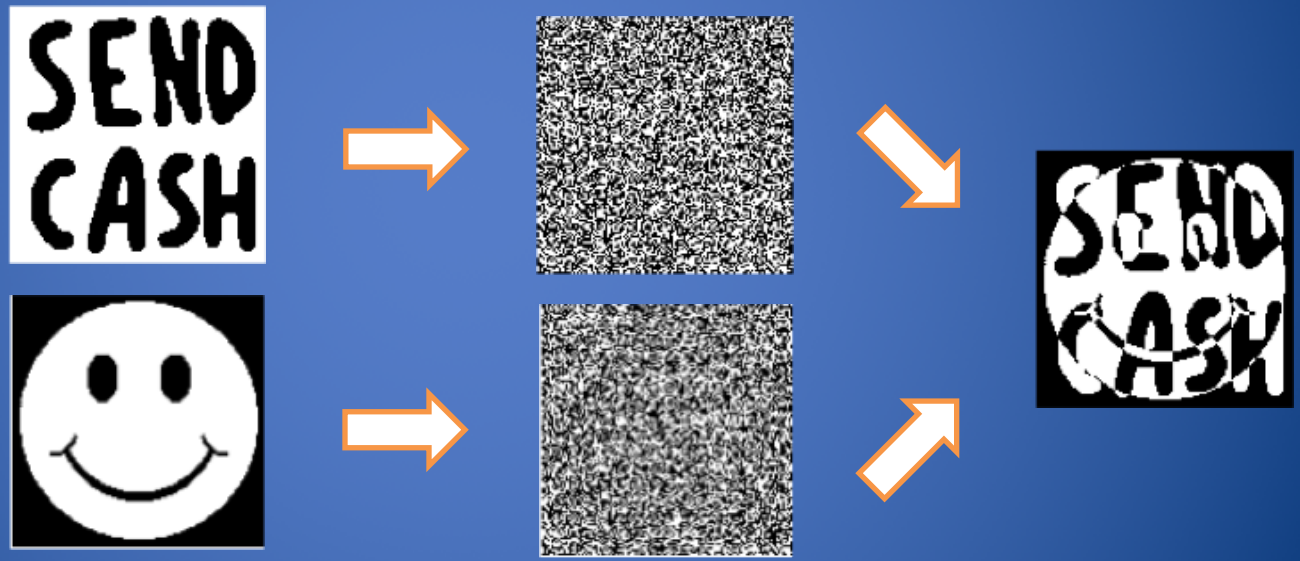
One-Time Pad

- Key
  - Sequence of random bits
  - Same length as plaintext
- Encryption
  - $C = K \oplus P$
  - Example
    - P = 01101001
    - K = 10110010
    - C = 11011011
- Decryption
  - $P = K \oplus C$

- Advantages
  - Each bit of the ciphertext is random
  - Fully secure if key used only once
- Disadvantages
  - Key as large as plaintext
    - Difficult to generate and share
  - Key cannot be reused

Pitfalls with One-Time Pads

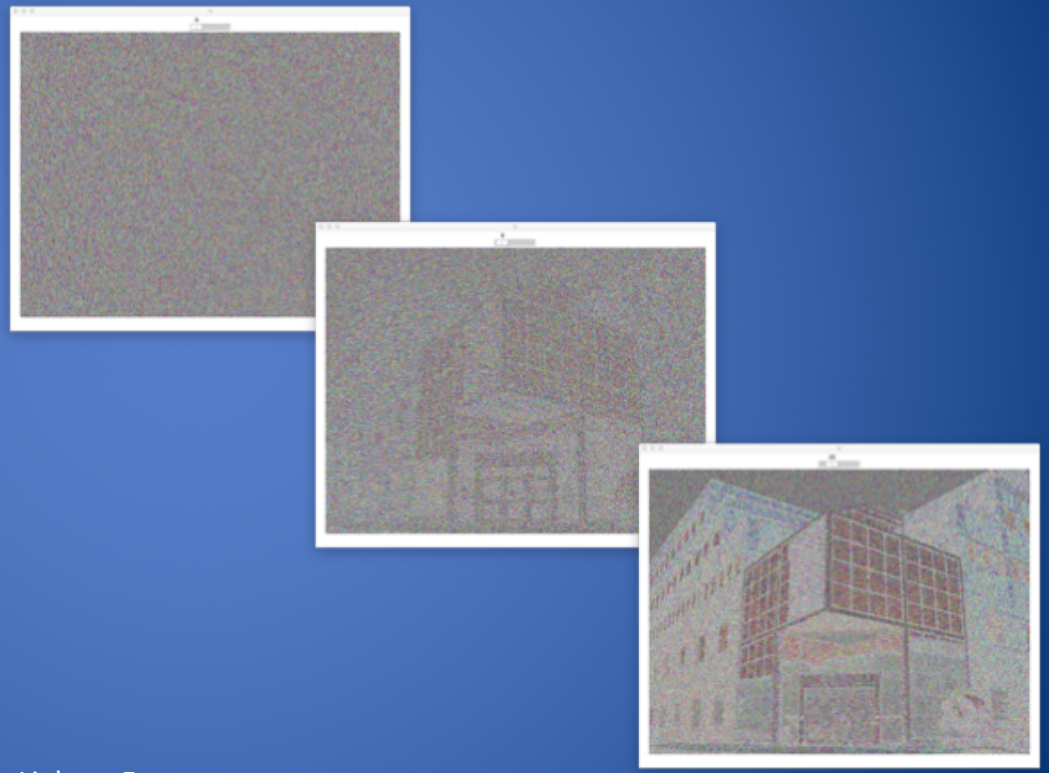
Key reuse



Source: Cryptosmith and David Lowry-Duda, Cryptography Stack Exchange

Pitfalls with One-Time Pads

Imperfect randomness



Source: Justin Bisignano and Joshua Liebow-Feeser

Modern Symmetric Encryption

Modern Symmetric Encryption

Data Encryption Standard (DES)

- Developed by IBM in collaboration with the NSA
- Became US government standard in 1977
- 56-bit keys
- Exhaustive search attack feasible since late 90s

Advanced Encryption Standard (AES)

- Selected as US government standard in 2001 through open competition
- 128-, 192-, or 256-bit keys
- Exhaustive search attack not currently possible

Image source: https://www.nsa.gov/resources/everyone/digital-media-center/image-galleries/places/

What We Have Learned

- Security goals and attacks on communication
- Frequency analysis defeats classic encryption
- One-time pads and the importance of randomness
- Use AES (not DES) for symmetric encryption