Introduction to the Basics of Cryptography

Anthony Kosednar

My Background

- Education
  - Number Theory, Field Theory, Cryptography and Statistics while in Highschool @ ASU
  - Studied Aerospace Engineering - Astronautics @ ASU
  - DHS Cybersecurity Training for Industrial Control Systems – SCADA, DCS, PLC, Embedded Control
  - GIAC Exploit Researcher and Advanced Penetration Tester - GXPN
- Part of these groups:
  - InfraGard
  - North American Network Operations Group (NANOG)
  - American Institute of Aeronautics and Astronautics (AIAA)
  - National Society of Professional Engineers (NSPE)
- I work in doing mainly cybersecurity for critical infrastructure
  - In the past consulted for sporting venues and large events (Arizona Cardinals, Arizona Board of Tourism, NFL, Super Bowl XLIX, Fiesta Bowl)
  - Currently work for a large publicly traded company

What is encryption used for?

- **Wireless connection**
- **Hard drives and flash drives**
- **Internet encryption**
- **Email encryption**
- **Hashing (technically not encryption…)**

Examples


```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1

mQINBFeyOyMBEACuzZ6NhyJuI/O/mdRGUdIPG8L7csViwxO5RIA+QruzC+s/6f0m
EY1nFVJr2kwuaO1C6rRsqn4OP3S4JgVLDOtdUICmCYydR0KXfAcOa3p4PKQ3pOWY
+r7xXrkaBTOcvKrrOM8P04GODxU6QdztXIG7XS109Cxn5NpIEze40Z2py/6E4wVf
h8FnvcksSiJi87pLxVMla/uYlRb9EIEZZNH+UYgBb9m3BAjAJfzySqJUhv8qehsO
R9HWEYFiiDOFkfPSNpuAnYraWGDTvqzSW1pgyXEorMR+9dhmkVxk0PCQXwDNGtJP
U6ulFWkJKDLDqRT4lhWV7FEcl1pZzZLxSBunqTTp62T72moc2MyWBEdBDXM18Ihk
QFBdSGI4yy4S4JAisKWolJPtD/n4TdBCY2jeVTVo29GfH3CR7lr84RoXL9wQ0RF5
5xAC/0IwYfxvzHSa291UkkUMe0eEkpfVU2EKnKVOgKnQlKq46q11CeznpBXbF11t
hLky63Z/TIPMkk/IHiTEKa4H+7UdxOK/NZ0KcHxhzBvTITzfn0mGQq5O1N0u9Cq1
BNNO3DBvJH125WreV/EKQWeP7y9/HCF5dz7UYTmRRaLcmEDuj5v/Wkio9Di1w5mZ
tlgwN6c3HSxH5JiyH0m3RsB/w7GhENeZH7X1205thkata9xF5gjwhtd74QARAQAB
tC1BbnRob255IEtvc2VkbmFyIDxhbnRob255Lmtvc2VkbmFyQGdtYWlsLmNvbT6J
AjgEEwEIACwFAleyOyMJEKs3HWt8d0hGAhsDBQkeEzgAAhkBBAsHCQMFFQgKAgME
FgABAgAAJwMP/0kYebLK8l2/0ewlTcgu0Twlik46FXHnGZmv8ct7MHrhAnSCrDFT
TppdD4sFIShdIoLSPmQtp6slcws4MdZf4R19RPmjILnWXIihvbUnhDgKRA7vgrxW
n1aGcamECvfM2OJOogTBF/E+ebGCwdqGcJperS1A83+02K0E0ffllBJGaq2P/2VP
4xLXCUsQOe6WCdhIgu741oz09MV0IQDnR0VZvEOSAxf03Nw4lds9qeREkwK2iEnb
E7/RrWdNwQLnLgr7pHXrPGv5tYmLozTMo5x3v6IBmz7rsf7KJRAVMx1kpJTe1oPp
7P9cVFvkryWkqvZqupcwHLQYJWwX02626KR2VlXQ2UCutVvj4kpvI3118RW8cbnV
I+EgO4HrrmAP8JPLoDQR01Pe49diSf8Fr7jlYfVTA2L7UKN7ndwmMLJpr3vHml1j
EkPozHasaIHFkAUKVJyolsYKZQSWSV3Nnle0relNZCsmFBwEdtVJFhz8Yj1s0akL
wAp4CNVTPR+JJm4oRlBWOw5NXAHpdYMTu3mLNvfg23pi2iN7Q2iKuyW1Bq+nr5ep
NY3r86i07GNAmlPYM8tFR2zLD9ck1jTzKWncKkkPn/X1fQBWtENvVc/dWW+YH8AU
SyZxp3TiLmL2HNws4UYwKYM9KyvjUhSvgFXa9kds3PLyqTYLi880HF4puQINBFey
OyMBEADJ9pHDGbWqEk1kGGeHu6MDbv1RT0Wdo7P2UQzIccOH/R2hAv0eSmFJkaON
QNqDaXiIkDKtm9hlzMwktlc1blegWdC8PlBlRcYTqAN6l4PigYGZ+RkeJFzMx0KY
23cTs0MWCOYWTKtj/DRr6tJbc9nIOZPJkapk1vVsLHFtK0S1XjTxcPSmsOfP7iIE
n63ks11wwUnufOXniUBgtwBpiE3CUYF+0I0aRCoMqRl3JES6wq6UPNdlRKN6mpP2
bBU/EyHF2og1iM4a0W9eRwc/khSwLUEX9WVtQdBQibmuUbd8sZvjqFw8+8QEKe4v
KwKm4Rdrlca+G1wDmPClu5vuVd11zr1SX6+tAM6WKwSsMJt2Q6KqJEXNQ6u7F/3H
yhio/YlQSdnwNsN90FzkeSwMM0foGCZeAy2Ak+UtmBAvvv+d2sAj8ArHAfXxzgQg
```



Lily

Terminology

- Cryptography
  - Practice and study of secure communication in the presence of third parties
- Key
  - A piece of information (parameter) that determines the functional output of a cipher
- Key space
  - Set of all possible keys used to generate a key
- Plaintext (cleartext)
  - Data unprotected by cryptographic means
- Ciphertext
  - Result of encryption performed on plaintext using a cipher

Terminology

- Algorithm
  - A finite list of well-defined instructions for calculating a solution
- Encryption
  - Using a cipher to transform plaintext into ciphertext
- Decryption
  - Using a cipher to transform ciphertext into plaintext
- Cipher
  - An algorithm for performing encryption and decryption
- Placeholder names
  - Alice, Bob, Eve (Eavesdropper), and Mallory (Malicious Attacker / Man-in-the-Middle)

Terminology

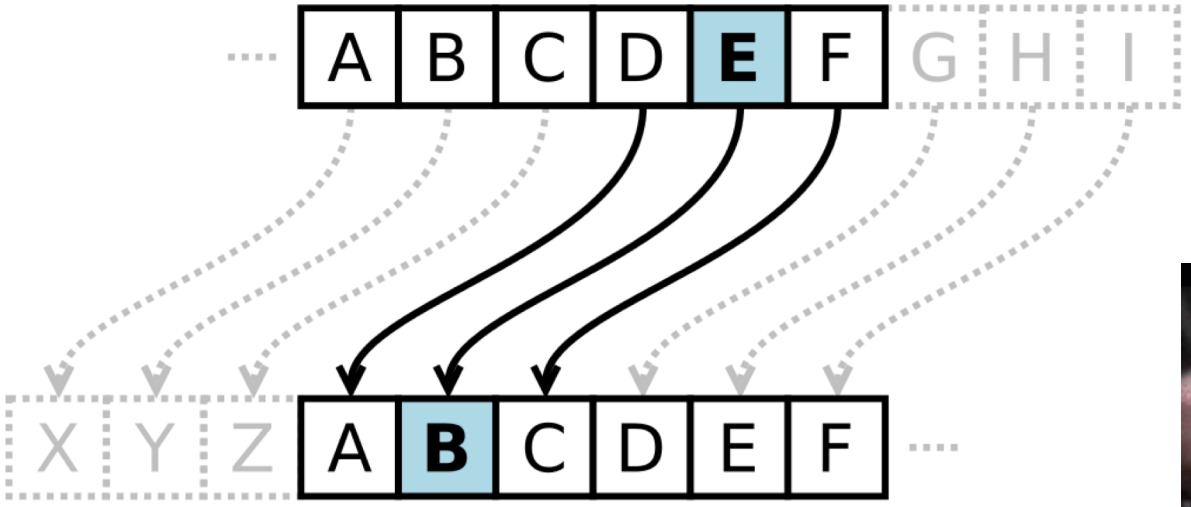
- Brute-force attack
  - Attempt all combinations of a key until the correct key is found
- Cipher suite
  - Combination of authentication, encryption, key exchange, and MAC algorithms
- Cryptographic system (cryptosystem)
  - A combination of cryptographic algorithms implementing a service (key generation, encryption, decryption)
- Cryptanalysis
  - The study of breaking, subverting, or bypassing cryptographic systems
- Steganography
  - Concealing a message, image, or file within another message, image, or file

Crypto History!

- Original goal of cryptography: confidentiality
- Typical Use: military communications and intelligence
  - **Substitution cipher:** Characters in plaintext are replaced with another character
  - **Transposition cipher:** Characters in plaintext are rearranged according to a regular pattern
  - Modern cryptography and cryptanalysis begins with WWII and the Enigma machine

Example: Caesar Cipher

- Shift each letter in the alphabet to the left by 3 spaces



- Example
  - Plaintext: SECURITY
  - Ciphertext: VHFXULWB

Rotation Ciphers

- The Caesar Cipher a specific subset of a substitution cipher, known as a rotation cipher
- All rotation ciphers are substitution ciphers
- A rotation cipher is noted by “ROT-#” where ‘#’ = the number of characters to shift when substituting

Cipher Concepts

- Describe the previous example, in cryptographic terminology
  - Algorithm: Replace each symbol in the message with the symbol three places to the left (23 to the right)
  - Cipher: The Caesar (rotational) Cipher, which is a specific variant of a substitution cipher
  - Key: The key is 23 (also known as ROT-23)
  - Key space: The key space is 26, since you have 26 options in how far to shift things before you loop around
    - ROT-26 doesn’t make for particular effective encryption

Substitution Cipher

Standard Alphabet

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
T	D	F	P	L	M	I	K	J	N	U	H	B	Y	G	V	C	X	Q	A	W	S	X	E	O

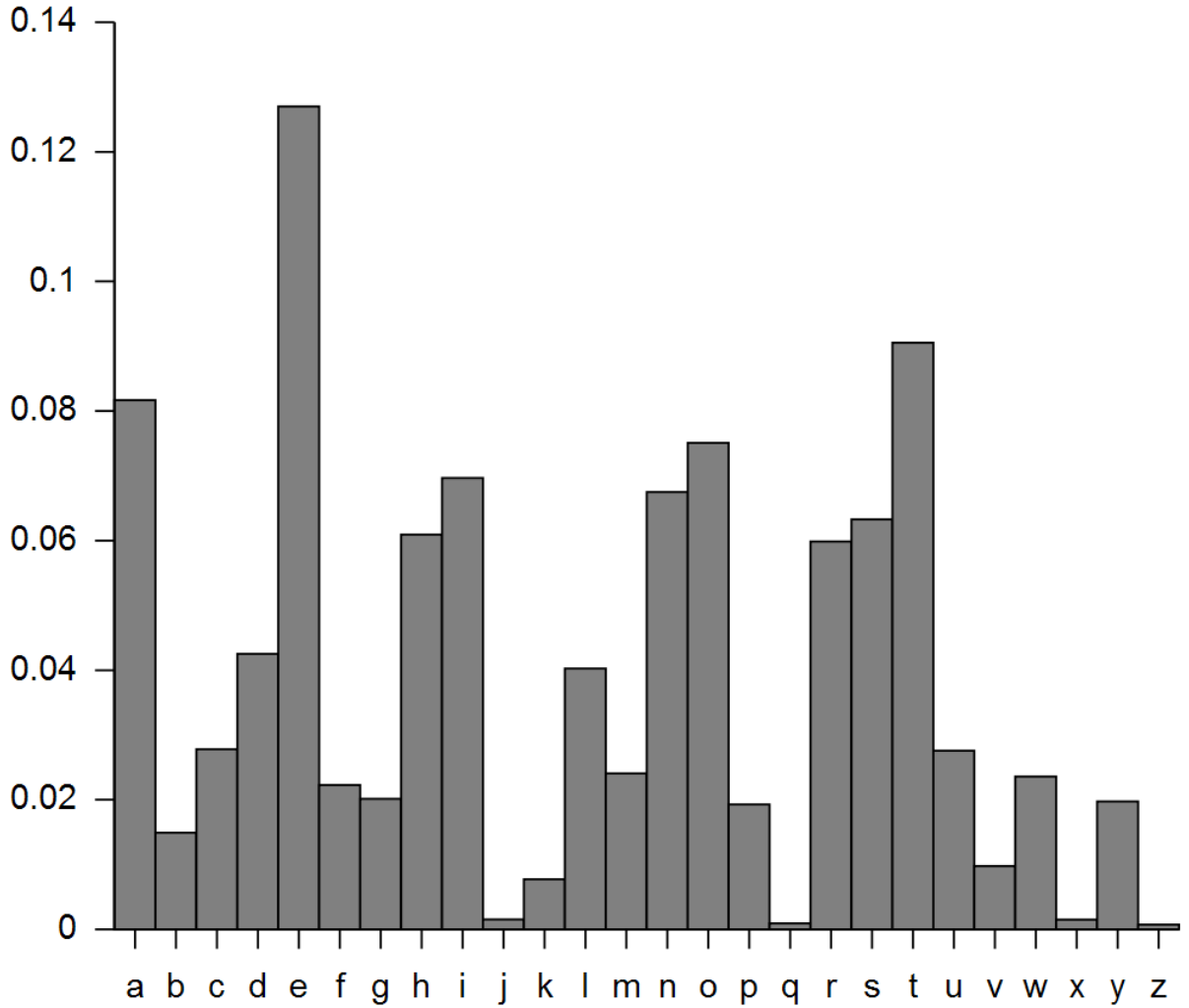
Cryptographic Alphabet

SECURITY = QLFWXJAO

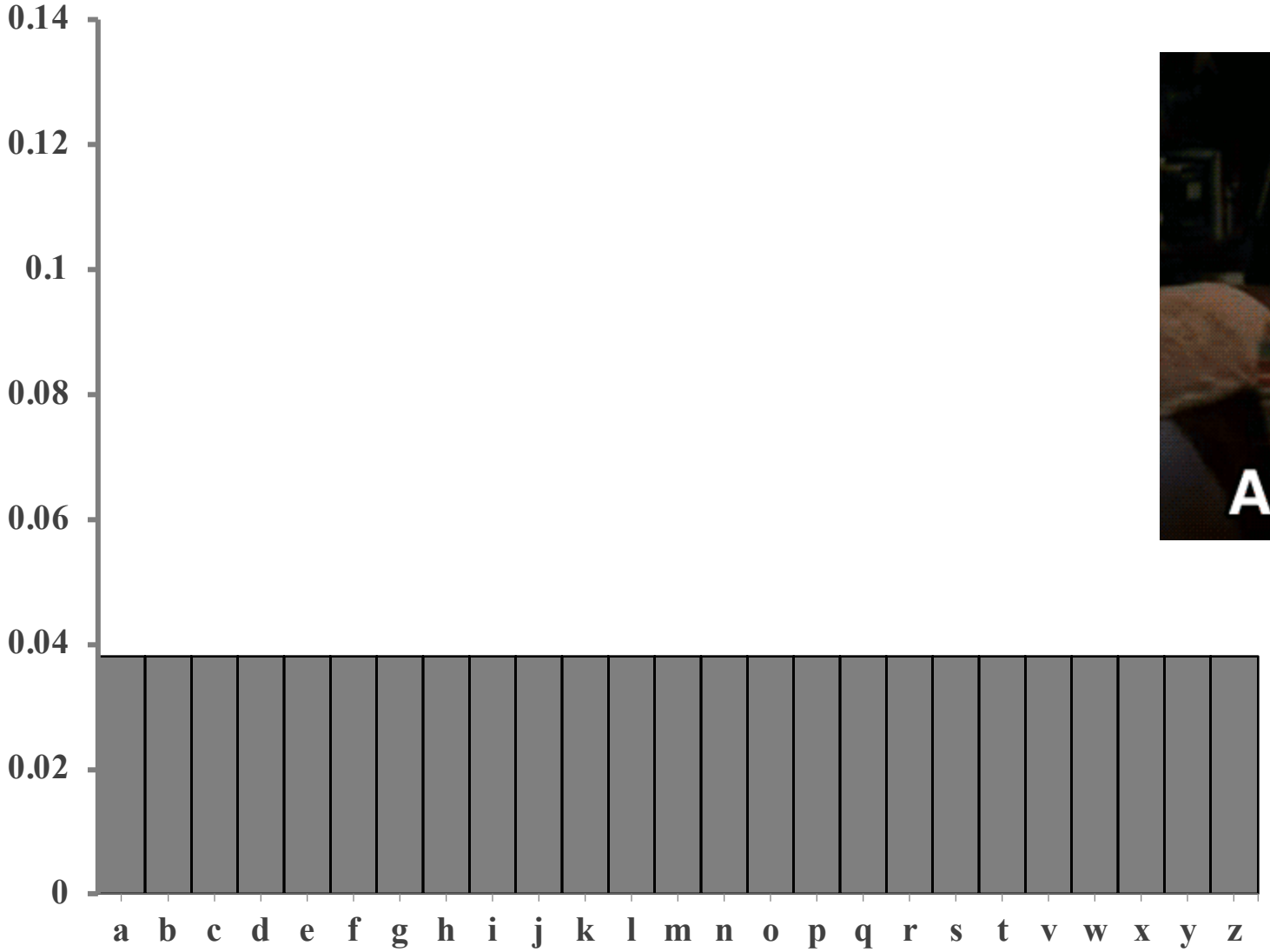
Frequency Analysis

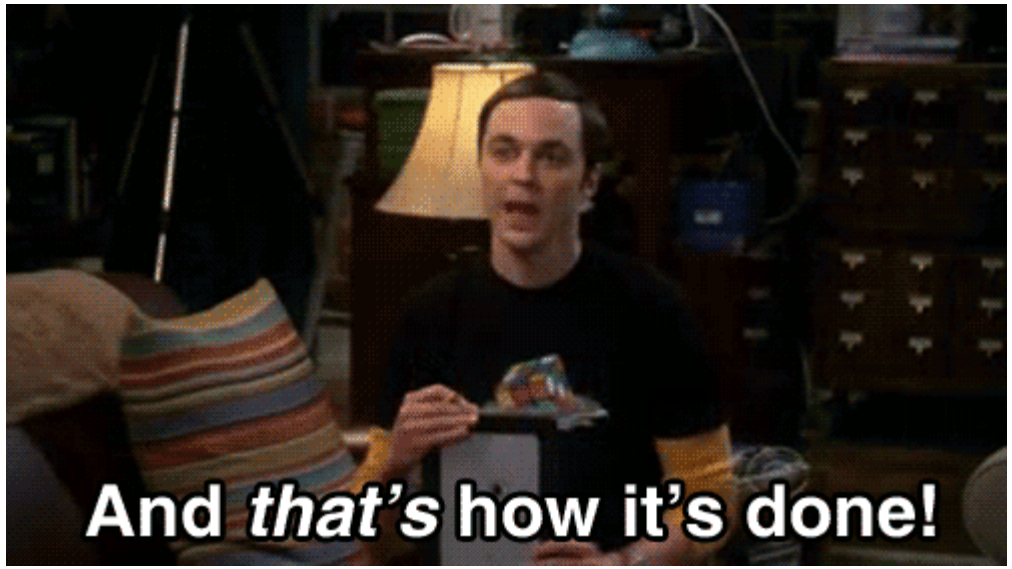
- Frequency analysis uses frequency of letters of the cipher text and the suspected plaintext
- Classical ciphers in general are vulnerable
- Simple substitution ciphers are highly vulnerable to frequency analysis

English letter usage frequency



Strong encryption letter frequency





Polyalphabetic Substitution

- Polyalphabetic Substitution
  - Substitution cipher with multiple alphabets
- Vigenère polyalphabetic Cipher
  - First described in Italy in 1553, and considered “the indecipherable cipher” until 1863
- Defeats frequency analysis
- Attempts to improve the Vigenère cipher eventually lead to the development of the one-time pad

Vigenère Cipher Example

Standard Alphabet	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Substitution set "A"	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Substitution set "B"	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
Substitution set "C"	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
Substitution set "D"	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
Substitution set "E"	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
Substitution set "F"	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
Substitution set "G"	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
Substitution set "H"	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
Substitution set "I"	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
Substitution set "J"	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
Substitution set "K"	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
Substitution set "L"	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
Substitution set "M"	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
Substitution set "N"	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
Substitution set "O"	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
Substitution set "P"	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Substitution set "Q"	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
Substitution set "R"	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
Substitution set "S"	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
Substitution set "T"	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
Substitution set "U"	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
Substitution set "V"	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
Substitution set "W"	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
Substitution set "X"	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Substitution set "Y"	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Substitution set "Z"	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Plaintext:	ATTACK AT DAWN
Key Word:	CRYPT OCRYP TOCRY
Cipher Text:	**CKRPVY CK BPPB**

Transposition (a.k.a. Permutation)

- Letters of plaintext are rearranged to produce cipher text
- Decipher by reversing the rearrangement process
- Route cipher transposition example
  - Plaintext: **abort the mission, you have been spotted**
  - Canonicalize: 5x7 grid, write downward from upper left
  - **Key (route): Down each column**
  - **Cipher text: ATSYV NTBHS OESEO EIUBP DRMOH EOXTI NAETX**
  - Key (route): spiraling inwards counter-clockwise from the bottom right
  - Cipher text: XTEAN ITROB ATSYV NTEDX OEHOM EHSOE SPBUI
- Modern symmetric ciphers use both substitution and transposition at the bit and byte level

A	B	O	R	T
T	H	E	M	I
S	S	I	O	N
Y	O	U	H	A
V	E	B	E	E
N	S	P	O	T
T	E	D	X	X

XOR (exclusive or)

- XOR "$\oplus$" (exclusive or) is a binary operator that is true only if one element is true

Input A	0	0	1	1
Input B	0	1	0	1
Output	0	1	1	0

- While it might seem simple or trivial, an entire encryption scheme (one-time pad) uses only XOR

One-time Pad

- The one-time pad (OTP) was invented by Frank Miller in 1882
- The only form of unbreakable cryptography
  - With a truly random key at least as long as the plaintext, you can combine the key with the plaintext to create a message that can never be decrypted
- The key can never be reused, hence “one-time”
- The key length requirement makes it infeasible for general use

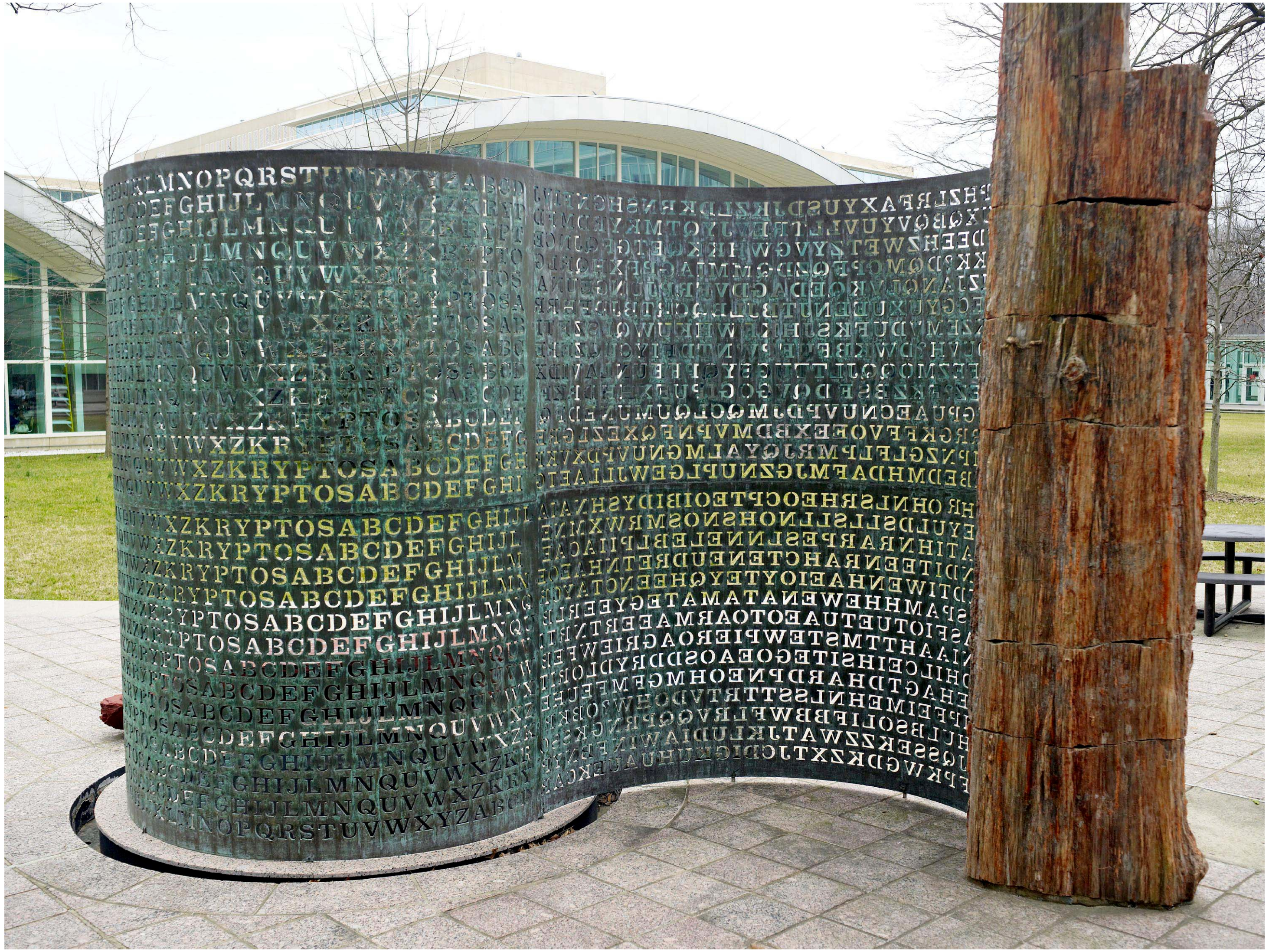
Steganography

- The art of concealing messages inside other mediums; these messages will appear innocuous
- Likely older than cryptography itself
  - Classic example is that of invisible ink
  - Modern examples include digital watermarking, hidden printer codes, or using images for data exfiltration
- Can be combined with cryptography
  - Especially common in places where the use of cryptography is illegal
  - Useful for avoiding the attention of authorities, as plainly visible encrypted messages may draw attention

Kerckhoff's Principle

- Auguste Kerckhoff, 1883
  - Direct translation
    - "The system must not require secrecy and can be stolen by the enemy without causing trouble"
  - Rephrased
    - "A cryptosystem should be secure even if everything about the system, except the key, is public knowledge"
  - This is in contrast to the common approach of "security through obscurity", where the security depends on people not knowing what the security measures are or how they work

Now you know how ¾ of the algorithms used



Questions??

Anthony.Kosednar@gmail.com