Cryptography

Bo Luo
bluo@ku.edu

Topic in Cryptography

- Basic Concepts
- Classical cryptography
- Modern cryptography
  - DES
  - AES
  - RSA

Elementary Cryptography

Introduction

Elementary Cryptography

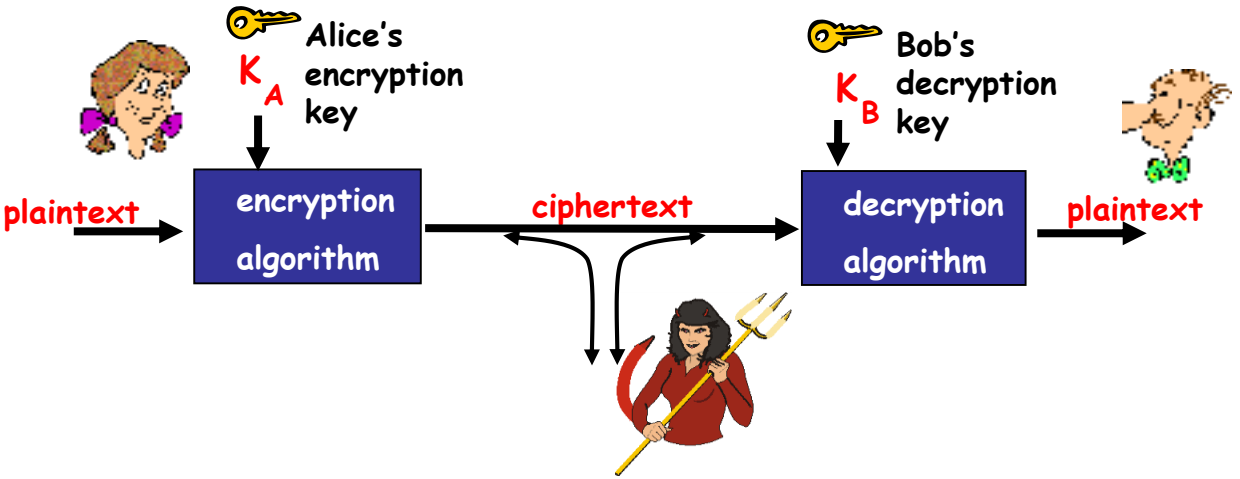
- Cryptography: an important tool
- Rooted in some heavy-duty math
  - number theory
  - group & field theory
  - computational complexity
  - probability
- Our goal:
  - be able to intelligently *use* crypto
  - not design/break cryptosystems

Security Goals

- **Confidentiality**: only sender, intended receiver "understand" message contents
  - sender encrypts message
  - receiver decrypts message
- **Message integrity**: sender, receiver want to ensure message not altered (in transit, or afterwards) without detection
- **End-point authentication**: sender, receiver want to confirm identity of each other

Terminology

- Cryptography: encipherment, digital signature, authentication exchange, …
  - S: sender (Alice)
  - R: recipient (Bob)
  - O: outsider or intruder
    - Chuck; Eve: eavesdropper; Mallory: malicious attacker
  - O might try to: block intercept modify fabricate



Terminology

- Cryptosystem
  - *Cryptographic algorithm* (a.k.a. *cipher*): algorithm(s) that take a *key* and convert *plaintext* to *ciphertext* and back.
    - The algorithm(s) used for encryption and decryption.
  - Cryptosystem:
    - cryptographic algorithm
    - set of all possible plaintexts
    - set of all possible ciphertexts
    - set of all possible keys

Terminology

- Cryptosystem
  - Mathematic representation of cryptosystem:
    - $K = \{0, 1\}^l$
    - $P = \{0, 1\}^m$
    - $C' = \{0, 1\}^n, C \subseteq C'$
    - $E : P \times K \rightarrow C$
    - $D : C \times K \rightarrow P$
    - $\forall p \in P, k \in K : D(E(p, k), k) = p$
    - It is infeasible to find $F : P \times C \rightarrow K$

Terminology

- Cryptosystem
  - You need to know:
    - Plaintext: P (characters? numbers? bits?)
    - Ciphertext: C
    - Encryption (encipher):

$$C = E(P)$$

    - Decryption (decipher):

$$P = D(C) = D(E(P))$$

Terminology

- Cryptology: Cryptography + Cryptanalysis
- *Cryptanalysis* is the study of methods for obtaining the meaning of encrypted information *without* accessing the secret information
  - "hacking"

Cryptography and Cryptanalysis

- A good cryptosystem should be infeasible to
  - enumerate *all* possible keys
  - find the key from any reasonable amount of ciphertext and plaintext by enumerating possible keys
  - produce plaintext from ciphertext without the key
  - distinguish ciphertext from true random values

Cryptography and Cryptanalysis

- What should be kept secret?
  - Keys
  - Cipher algorithms

Cryptography and Cryptanalysis

- Restricted Algorithms
  - Algorithm itself is secret
  - *Security* of algorithm relies on its *secrecy*
- Not good practice:
  - can't be used by large or changing group
  - if one accidentally reveals the algorithm, everyone must change
  - different groups need different algorithms
  - it is difficult to design (and prove) good algorithms
  - people who designs the cipher != people who use the cipher

Cryptography and Cryptanalysis

- Kerckhoffs' Law
  - "The system must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience."
  - *Secrecy* must reside entirely with the *key*
  - must assume that the enemy has complete details of the cryptographic algorithm
  - enemy will reverse engineer your algorithm

Cryptography and Cryptanalysis

- *Cryptanalysis* is the study of methods for obtaining the meaning of encrypted information *without* accessing the secret information
  - Need knowledge of the general characteristics of plaintext or knowledge of some sample plaintext-ciphertext pairs
  - *Ciphertext only*
    - *Search over keys, recognizable plaintext, enough ciphertext*
  - *Known plaintext*
  - *Chosen plaintext*

Cryptography and Cryptanalysis

- Goal of cryptanalysis: break the algorithm
  - *Total break* - find the key K such that D(K,C)=P
  - *Global deduction* - find alternative algorithm, A, equivalent to D(K,C) without knowing K
  - *Instance (or local) deduction* - find the plaintext of an intercepted ciphertext
  - *Information deduction* - get some information about the key or plaintext
    - first bits of the key,
    - info about the form of the plaintext, …

Cryptography and Cryptanalysis

- Definition of Security
  - Unconditional secure
    - If the ciphertext does not contain enough information to uniquely determine the plaintext
    - No matter how hard the opponent tries
    - One-time pad
  - Computational secure
    - If the cost of breaking the cipher exceeds the value of encrypted data
    - If the time needed to break the cipher exceeds the lifetime of data

Cryptography and Cryptanalysis

- **Brute-Force Attack**
  - Try every possible key on ciphertext until getting an intelligible translation into plaintext
  - On average, try half of the keys
  - Costly when key space is large
  - Remember *Moore's Law*

Key size (bits)	Number of alternative keys		Time required at 1 decryption/*ms*		Time required at 10^6 decryption/*ms*
32	2^{32}	= 4.3×10^9	2^{31} *ms*	= 35.8 minutes	2.15 milliseconds
56	2^{56}	= 7.2×10^{16}	2^{55} *ms*	= 1142 years	10.01 hours
128	2^{128}	= 3.4×10^{38}	2^{127} *ms*	= 5.4×10^{24} years	5.4×10^{18} years
168	2^{168}	= 3.7×10^{50}	2^{167} *ms*	= 5.9×10^{36} years	5.9×10^{30} years
26 characters (permutation)	26!	= 4×10^{26}	2×10^{26} *ms*	= 6.4×10^{12} years	6.4×10^6 years

Cryptosystems

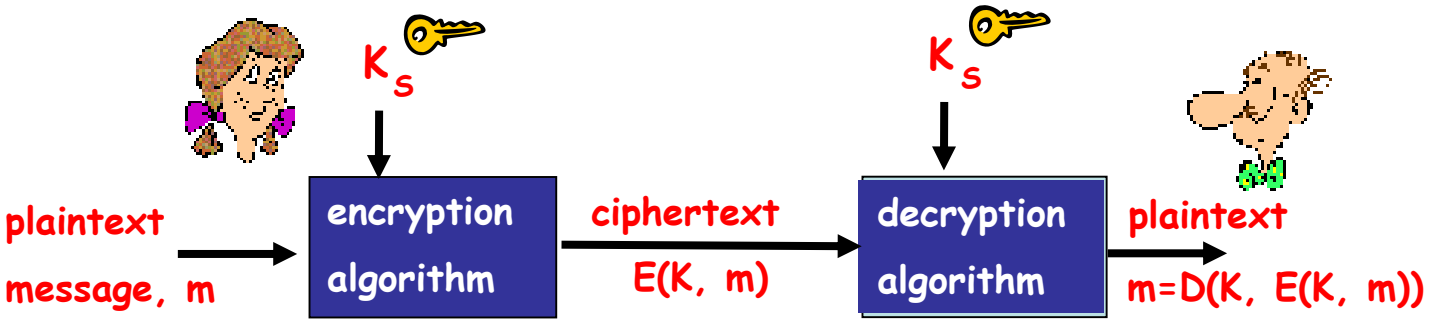
- Secret key cryptography
  - Involves the use *one* key
- Public key cryptography
  - Involves the use of *two (a pair of)* keys
- Hash functions
  - Involves the use of *no* key
  - Nothing secret: How can this be useful?

Cryptosystems

- Secret Key Cryptography
  - Bob and Alice share a same (symmetric) key
  - a.k.a. private encryption, single-key encryption, symmetric-key encryption ; or conventional encryption

$$C = E(K, P)$$

$$P = D(K, C) = D(K, E(K,P))$$



Cryptosystems

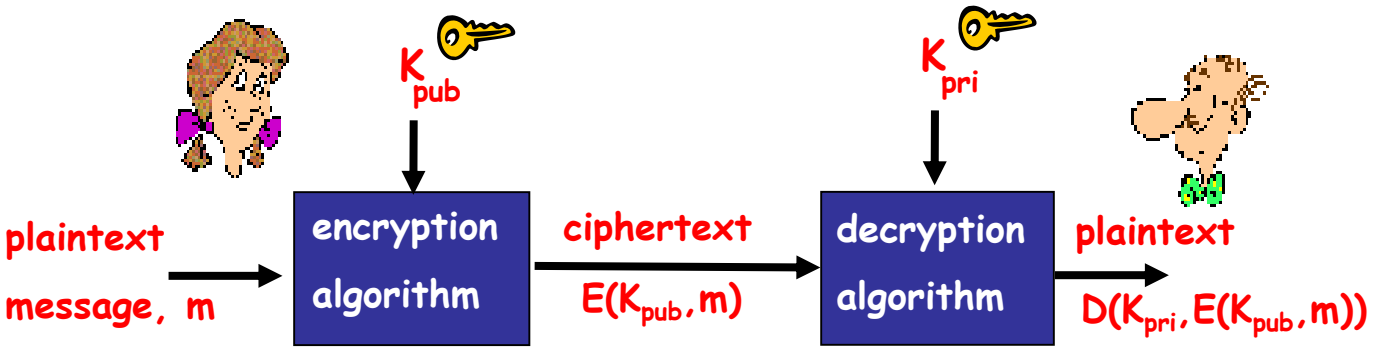
- Requirements for secret key cryptography
  - Encryption algorithm is publicly known
  - Secure use of symmetric encryption implies:
    - a strong encryption algorithm
    - a secret key known only to sender/receiver
  - Need a *secure channel* to distribute keys!

Cryptosystems

- Public Key Cryptography
  - a.k.a. asymmetric encryption
  - Bob has a pair of public and private keys
  - Bob's public key is known by Alice
    - Alice uses Bob's public key to encrypt the message

$$C = E(K_{pub}, P)$$

$$P = D(K_{pri}, C) = D(K_{pri}, E(Kpub, P))$$



Cryptosystems

- Cryptographic hash
  - Hash algorithms are known as *message digests* or *one-way transformations*
    - Fixed-length, condense and one-wayness
  - Password hashing: secure password storage
  - Message integrity: keyed hash
  - Message fingerprint: digest
  - Digital signature efficiency

Elementary Cryptography

Secret Key Cryptography

Caesar Cipher

- One of the oldest cryptosystems
- Caesar Cipher: Every character is replaced with the character three slots to the right.
- A very simple *shift cipher* or *substitution cipher*

  - Caesar: ATTACK AT FIVE
  - Ciphertext: DWWDFN DW ILYH

Caesar Cipher

- Break a Caesar Cipher
  - Too easy!
  - Let's try

URFN FKDON MDBKDZN

Caesar Cipher

- Formal definition
  - Encryption:

$$E_K(m) = m + 3 \bmod 26$$

  - Decryption:

$$D_K(c) = c - 3 \bmod 26$$

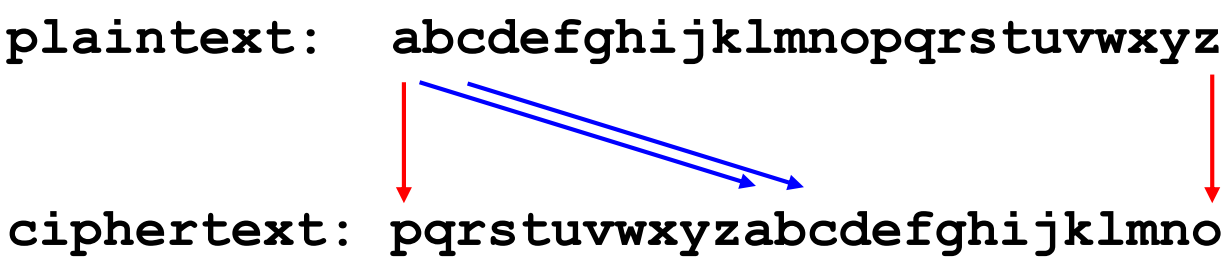
Shift Cipher

- Caesar cipher is a special case of *shift cipher*
- Shift cipher
  - Encryption:

$$E_K(m) = m + K \bmod 26$$

  - Decryption:

$$D_K(c) = c - K \bmod 26$$



Shift Cipher

- Break a shift cipher: still easy!
- Brute force: how many possibilities?
  - 26
  - Maybe just 25…

Shift Cipher

- Break a shift cipher: still easy!

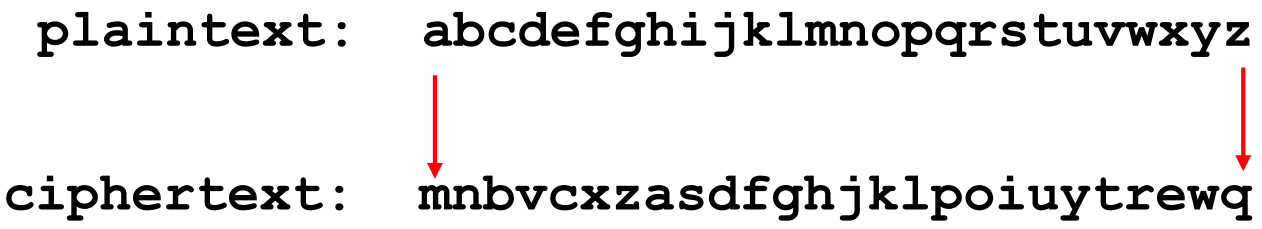
YHKMNGX PABVA ATL T ZKXTM WXTE HY IHPXK BG HMAXK FTMMXKL UNM XLIXVBTEER BG PTK VTG UKBGZ TUHNM ZKXTM VATGZXL BG T LBMNTMBHG MAKHNZA OXKR LEBZAM YHKVXL

Substitution cipher

- Shift cipher is a special case of *substitution cipher*
- Substitution cipher is to substitute one thing for another
  - Monoalphabetic cipher: substitute one letter for another
  - Key: the mapping from the set of 26 letters to the set of 26 letters

Substitution cipher

- Monoalphabetic cipher: substitute one letter for another



  - Alice: Hello Bob
  - Ciphertext: ACGGK NKN

Substitution cipher

- Another monoalphabetic cipher: keyword mixed alphabet
  - Key: Jayhawk

```
plaintext:   abcdefghijklmnopqrstuvwxyz
ciphertext:  jayhwkbcdefgilmnopqrstuvxz
```

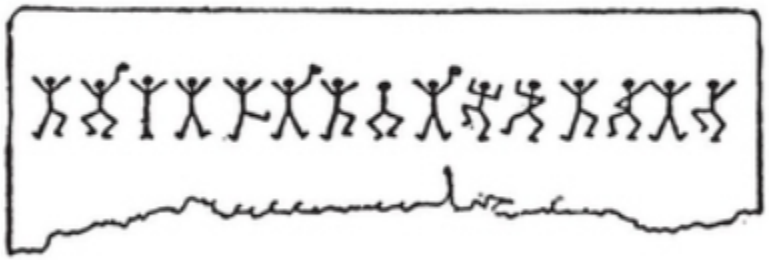
Substitution cipher

- Breaking the monoalphabetic cipher
- Brute force attack
  - How many possible substitution alphabets?
    - $26! \approx 4 * 10^{26}$
  - Can we try all permutations?
    - 10^9 tests per second
    - 10K nodes
    - How much time do we need? $4 * 10^{13}$ seconds ~ $3 * 10^7$ years
  - How to reduce it?

shift cipher is 25 ——>substitution is 26!

Substitution cipher

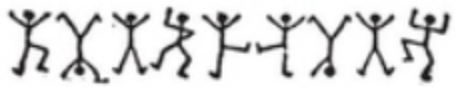
Holmes held up the paper so that the sunlight shone full upon it. It was a page torn from a notebook. The markings were done in pencil, and ran in this way:



Holmes examined it for some time, and then, folding it carefully up, he placed it in his pocketbook.

Substitution cipher

the table. Here is a copy of the hieroglyphics:



"Excellent!" said Holmes. "Excellent! Pray continue."

"When I had taken the copy, I rubbed out the marks, but, two mornings later, a fresh inscription had appeared. I have a copy of it here":

Holmes rubbed his hands and chuckled with delight.

"Our material is rapidly accumulating," said he.

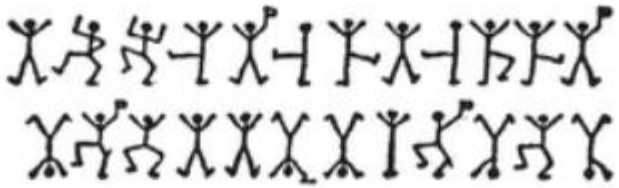
Substitution cipher

"Have you that fresh drawing?"

"Yes, it is very short, but I made a copy of it, and here it is."

Again he produced a paper. The new dance was in this form:

He inclosed a copy of it, which is here reproduced:



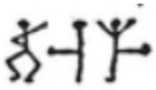
Substitution cipher

"Having once recognized, however, that the symbols stood for letters, and having applied the rules which guide us in all forms of secret writings, the solution was easy enough. The first message submitted to me was so short that it was impossible for me to do more than to say, with some confidence, that the symbol  stood for E. As you are aware, E is the most common letter in the English alphabet, and it predominates to so marked an extent that even in a short sentence one would expect to find it most often. Out of fifteen symbols in the first message, four were the same, so it was reasonable to set this down as E. It is true that in some cases the figure was bearing a flag, and in some cases not, but it was probable, from the way in which the flags were distributed, that they were used to break the sentence up into words. I accepted this as a hypothesis, and noted that E was represented by 

Substitution cipher

"But now came the real difficulty of the inquiry. The order of the English letters after E is by no means well marked, and any preponderance which may be shown in an average of a printed sheet may be reversed in a single short sentence. Speaking roughly, T, A, O, I, N, S, H, R, D, and L are the numerical order in which letters occur; but T, A, O, and I are very nearly abreast of each other, and it would be an endless task to try each combination until a meaning was arrived at. I therefore waited for fresh material. In my second interview with Mr. Hilton Cubitt he was able to give me two other short sentences and one message, which appeared — since there was no flag — to be a single word. Here are the symbols. Now, in the single word I have already got the two E's coming second and

Substitution cipher

fourth in a word of five letters. It might be 'sever,' or 'lever,' or 'never.' There can be no question that the latter as a reply to an appeal is far the most probable, and the circumstances pointed to its being a reply written by the lady. Accepting it as correct, we are now able to say that the symbols  stand respectively for N, V, and R.

Substitution cipher

"Even now I was in considerable difficulty, but a happy thought put me in possession of several other letters. It occurred to me that if these appeals came, as I expected, from someone who had been intimate with the lady in her early life, a combination which contained two E's with three letters between might very well stand for the name 'ELSIE.' On examination I found that such a combination formed the termination of the message which was three times repeated. It was certainly some appeal to 'Elsie.' In this way I had got my L, S, and I. But what appeal could it be? There were only four letters in the word which preceded 'Elsie,' and it ended in E. Surely the word must be 'COME.' I tried all other four letters ending in E, but could find none to fit the case. So now I was in possession of C, O, and M, and I was in a position to attack the first message once more, dividing it into words and putting dots for each symbol which was still unknown. So treated,

Substitution cipher

it worked out in this fashion:

.M .ERE ..E SL . NE .

"Now the first letter can only be A, which is a most useful discovery, since it occurs no fewer than three times in this short sentence, and the H is also apparent in the second word. Now it becomes:

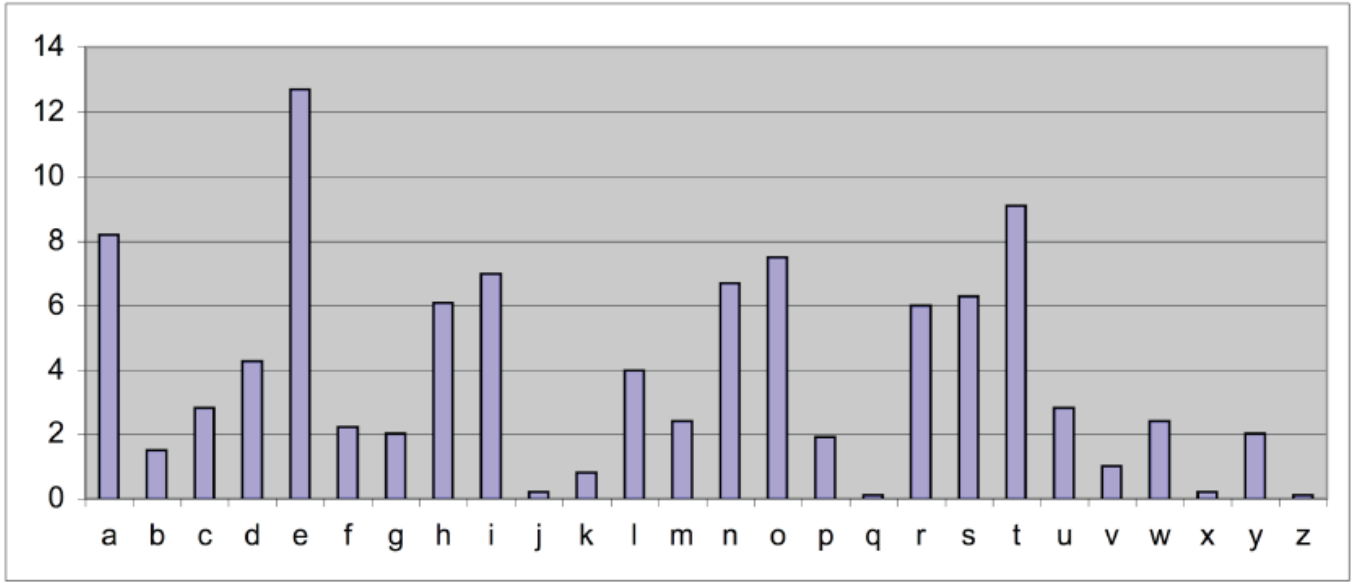
AM HERE A . E SLANE .

Or, filling in the obvious vacancies in the name:

AM HERE ABE SLANEY.

Substitution cipher

- Breaking the monoalphabetic cipher
- Frequency analysis
  - In English



Substitution cipher

- Breaking the monoalphabetic cipher
- Frequency analysis

Vg gbbx n ybg bs oybbq, fjrng naq grnef gb trg gb jurer jr ner gbqnl, ohg jr unir whfg ortha. Gbqnl jr ortva va rnearfg gur jbex bs znxvat fher gung gur jbeyq jr yrnir bhe puvyqera vf whfg n yvggyr ovg orggre guna gur bar jr vaunovg gbqnl.

It took a lot of blood, sweat and tears to get to where we are today, but we have just begun. Today we begin in earnest the work of making sure that the world we leave our children is just a little bit better than the one we inhabit today.

Substitution cipher

- Breaking the monoalphabetic cipher
  - Common English Digrams and Trigrams

Digrams	Trigrams
EN	ENT
RE	ION
ER	AND
NT	ING
TH	IVE
ON	TIO
IN	FOR
TF	OUR
AN	THI
OR	ONE

Substitution cipher

- Breaking the monoalphabetic cipher

GS SGU WL LS KZAVU YJAY JU WL GSY XWLYNZKUX KR LSPUYJWGO NGUQHUMYUX

  - Frequency analysis
  - U: 8; Y: 6; G: 5; S: 5; L: 5; W: 4; J: 3; K: 3; X: 3; A: 2; N: 2;

Substitution cipher

- Breaking the monoalphabetic cipher

GS SGE WL LS KZAVE YJAY JE WL GSY XWLYNZKEX KR LSPEYJWGO NGEQHEMYEX

  - Frequency analysis
  - U: 8 - E; Y: 6; G: 5; S: 5; L: 5; W: 4; J: 3; K: 3; X: 3; A: 2; N: 2;

Substitution cipher

- Breaking the monoalphabetic cipher

GS SGE WL LS KZAVE YJAY JE WL GSY XWLYNZKEX KR LSPEYJWGO NGEQHEMYEX

  - Frequency analysis
  - U: 8 - E; Y: 6; G: 5; S: 5; L: 5; W: 4; J: 3; K: 3; X: 3; A: 2; N: 2;
  - Frequent two letter words?

WL or LS

Substitution cipher

- Breaking the monoalphabetic cipher

GS SGE IS SS KZAVE YJAY JE
IS GSY XISYNZKEX KR
SSPEYJIGO NGEQHEMYEX

  - Frequency analysis
  - U: 8 - E; Y: 6; G: 5; S: 5; L: 5 - S; W: 4 - I; J: 3; K: 3; X: 3; A: 2; N: 2;
  - Frequent two-letter word?
  - SS → SO

Substitution cipher

- Breaking the monoalphabetic cipher

GO OGE IS SO KZAVE YJAY JE IS GOY XISYNZKEX KR SOPEYJIGO NGEQHEMYEX

  - Frequency analysis
  - U: 8 - E; Y: 6; G: 5; S: 5 - O; L: 5 - S; W: 4 - I; J: 3; K: 3; X: 3; A: 2; N: 2;
  - Frequent two-letter word?
  - What is G?

Substitution cipher

- Breaking the monoalphabetic cipher

NO ONE IS SO KZAVE YJAY JE
IS NOY XISYNZKEX KR
SOPEYJINO NNEQHEMYEX

  - Frequency analysis
  - U: 8 - E; Y: 6; G: 5 - N; S: 5 - O; L: 5 - S; W: 4 - I; J: 3; K: 3; X: 3; A: 2; N: 2;
  - Frequent two-letter word?
  - What is Y?

Substitution cipher

- Breaking the monoalphabetic cipher

NO ONE IS SO KZAVE TJAT JE
IS NOT XISTNZKEX KR
SOPETJINO NNEQHEMTEX

  - Frequency analysis
  - U: 8 - E; Y: 6 - T; G: 5 - N; S: 5 - O; L: 5 - S; W: 4 - I; J: 3; K: 3; X: 3; A: 2; N: 2;
  - Frequent two-letter word?
  - What is J? What is A?

Substitution cipher

- Breaking the monoalphabetic cipher

NO ONE IS SO KZAVE THAT HE IS NOT XISTNZKEX KR SOPETHINO NNEQHEMTEX

  - Frequency analysis
  - U: 8 - E; Y: 6 - T; G: 5 - N; S: 5 - O; L: 5 - S; W: 4 - I; J: 3 - H; K: 3; X: 3; A: 2 - A; N: 2;
  - Frequent two-letter word?
  - SOPETHINO → SOMETHING

Substitution cipher

- Breaking the monoalphabetic cipher

NO ONE IS SO KZAVE THAT HE IS NOT XISTNZKEX KR SOMETHING NNEQHEMTEX

  - Frequency analysis
  - U: 8 - E; Y: 6 - T; G: 5 - N; S: 5 - O; L: 5 - S; W: 4 - I; J: 3 - H; K: 3; X: 3; A: 2 - A; N: 2;
  - Frequent two-letter word?
  - ---EX → ER or ED or ES

Substitution cipher

- Breaking the monoalphabetic cipher

NO ONE IS SO KZAVE THAT HE IS NOT DISTNZKED KR SOMETHING NNEQHEMTED

  - Frequency analysis
  - U: 8 - E; Y: 6 - T; G: 5 - N; S: 5 - O; L: 5 - S; W: 4 - I; J: 3 - H; K: 3; X: 3 - D; A: 2 - A; N: 2;
  - Frequent two-letter word?
  - ---EX → ER or ED or ES

Substitution cipher

- Breaking the monoalphabetic cipher … is easy!
  - Cryptanalysts use properties of plaintext
  - What can be cryptographers' counter-moves?

Substitution cipher

- Breaking the monoalphabetic cipher … is easy!
  - Cryptanalysts use properties of plaintext
  - What can be cryptographers' counter-moves?

  - Polyalphabetic ciphers
    - use multiple alphabets
  - Homophonic ciphers
    - multiple possible output characters for an input character
  - Polygram ciphers
    - encipher groups of letters at once

Homework 1

- Posted on Bb
- Chapter 2 of text book.
- Exercise 1, 2, 3, 4, 5
- Only need to correctly decrypt 3 ciphertexts to earn full credit.

- Due: a week from today.

Vigenere Cipher

- Problem with monoalphabetic cipher?
  - One mapping scheme for the entire encryption process
  - Cryptanalysts could observe the patterns
- Countermeasure
  - Use a different mapping for each character in the plaintext

Vigenere Cipher

- The Vigenere Cipher
  - Construct a table (the Vigenere tableau)
  - Each row in table is a different shift (alphabet)
    - Why shift cipher instead of monoalphabetic substitution?
  - Sender and receiver agree on sequence of rows
  - Helps to disguise patterns

Vigenere Cipher

0	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
1	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
2	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
3	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
4	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
5	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
6	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
7	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
8	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
9	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
10	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
11	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
12	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
13	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
14	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
15	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
16	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
17	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
18	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
19	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
20	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
21	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
22	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
23	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
24	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
25	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

Vigenere Cipher

- The Vigenere Cipher
  - Alice and Bob agree on {5, 19, 7, 11, 21} as key
  - In encryption:
    - Encrypt letter 1 with row 5
    - Encrypt letter 2 with row 19
    - Encrypt letter 3 with row 7
    - Encrypt letter 4 with row 11
    - Encrypt letter 5 with row 21
    - Encrypt letter 6 with row 5
    - Encrypt letter 7 with row 19
    - Encrypt letter 8 with row 7

Vigenere Cipher

- Encrypt “superbowl” with K={5, 19, 7, 11, 21}
- Letter 1: S → X

0	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
1	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
2	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
3	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
4	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
5	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
6	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
7	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
8	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
9	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
10	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
11	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
12	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
13	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
14	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
15	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
16	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
17	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
18	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
19	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
20	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
21	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
22	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
23	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
24	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
25	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

Vigenere Cipher

- Encrypt “superbowl” with K={5, 19, 7, 11, 21}
- X
- Letter 2: U → N

0	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
1	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
2	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
3	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
4	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
5	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
6	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
7	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
8	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
9	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
10	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
11	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
12	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
13	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
14	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
15	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
16	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
17	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
18	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
19	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
20	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
21	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
22	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
23	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
24	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
25	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

Vigenere Cipher

- Encrypt “superbowl” with K={5, 19, 7, 11, 21}
- XN
- Letter 3: P → W

0	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
1	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
2	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
3	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
4	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
5	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
6	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
7	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
8	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
9	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
10	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
11	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
12	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
13	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
14	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
15	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
16	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
17	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
18	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
19	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
20	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
21	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
22	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
23	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
24	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
25	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

Vigenere Cipher

- Encrypt “superbowl” with K={5, 19, 7, 11, 21}
- XNW
- Letter 4: E → P

0	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
1	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
2	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
3	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
4	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
5	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
6	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
7	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
8	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
9	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
10	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
11	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
12	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
13	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
14	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
15	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
16	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
17	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
18	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
19	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
20	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
21	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
22	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
23	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
24	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
25	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

Vigenere Cipher

- Encrypt “superbowl” with K={5, 19, 7, 11, 21}
- XNWP
- Letter 5: R → M

0	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
1	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
2	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
3	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
4	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
5	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
6	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
7	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
8	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
9	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
10	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
11	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
12	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
13	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
14	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
15	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
16	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
17	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
18	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
19	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
20	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
21	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
22	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
23	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
24	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
25	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

Vigenere Cipher

- Rows: letters, not numbers
- Key: a phrase

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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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

Vigenere Cipher

- Encrypt “JAYHAWK” with “EECS”
- N

	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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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

Vigenere Cipher

- Encrypt “JAYHAWK” with “EECS”
- NE

	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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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

Vigenere Cipher

- Encrypt “JAYHAWK” with “EECS”
- NEA

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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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

Vigenere Cipher

- Encrypt “JAYHAWK” with “EECS”
- NEAZ

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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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

Vigenere Cipher

- Encrypt “JAYHAWK” with “EECS”
- NEAZE

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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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

Vigenere Cipher

- Encrypt “JAYHAWK” with “EECS”
- NEAZEA

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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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

Vigenere Cipher

- Encrypt “JAYHAWK” with “EECS”
- NEAZEAM

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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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

Vigenere Cipher

- Do we really need the table?
- Encrypt "JAYHAWK" with "EECS"
  - Letter 1: J + E mod 26
    - J + 4 mod 26 = N
  - Letter 2: A + E mod 26 = E
  - Letter 3: Y + C mod 26 = A

A 是0； A+任何字母就是本身

Vigenere Cipher

- Practice
  - Use K= “superbowl” to encrypt P = “rockchalkjayhawk”

Vigenere Cipher

- Practice
  - Use K= “superbowl” to encrypt P = “rockchalkjayhawk”
  - C = “jirotiohvbunlrxy”

Vigenere Cipher

- Problem with monoalphabetic cipher?
  - One mapping scheme for the entire encryption process
  - Cryptanalysts could observe the patterns
- Countermeasure
  - Use a different mapping for each character in the plaintext
- Breaking a Vigenere cipher
  - Difficult
  - First: find the key length
  - Could use brute forth attack to try all possible key lengths
  - For each key length, observe the distribution patterns.

Mini-project 1: Vigenere Cipher

- Implement a simple Vigenere Cipher
  - The plaintext/ciphertext should only contain letters
  - Assume valid input
  - Spaces in the plaintext should be removed.

  The algorithm for encryption is: $E_K(m) = m + K \bmod 26$
  The algorithm for decryption is: $E_K(m) = m - K \bmod 26$

- Your input/output should be text strings, with both uppercase and lowercase letters.
- Not case sensitive. That is, both "A" and "a" must be converted to "1" (or "0") in your program.

- **See more details at: Bb → Assignments**

Mini-project 1: Password Cracker

- Three parameters: (1) string ciphertext; (2) integer *keyLength*; and (3) an integer *firstWordLength:* the length of the first word of the plaintext.
- Test every possible key that has the length of *keyLength*: from all "A"s to all "Z"s.
  - You cannot exploit the dictionary to guess the key, since the key may not be a valid word.
- For each key candidate, generate a "plaintext", and compare it with the dictionary.
  - Only need to check if the first word is a valid word in the dictionary.
  - If Yes, display the plaintext and the key. However, do not stop, as the "plaintext" might be wrong.
- Efficiency is very important in evaluating each "plaintext" candidate.

- **See more details at: Bb → Assignments**

Homophonic Ciphers

- Try to hide plaintext patterns (statistics)
- Map each plaintext character to any of a set of ciphertext characters
- *Homophones* : set of possible ciphertext characters that map to a single plaintext character.

Homophonic Ciphers

- Homophonic Ciphers

Plaintext	Homophones
A	624, 18, 329, 19, 4
B	5, 333, 511
C	919, 14, 67, 83
D	414, 30, 238, 71, 15, 6
E	8, 13, 12
F	61, 422
G	413, 2, 16

- Encrypt: CAFE: 14 624 6 12

61 2 wrong answer

Homophonic Ciphers

- Q1: How many homophones per plaintext character?
  - Choice 1: fixed number
  - Choice 2: variable: more for frequent plaintext characters
  - Which is better, why?
- Q2: Are there disadvantages to this?
  - Inefficient: ciphertext longer than the plaintext

Polygram Ciphers

- Monoalphabetic ciphers and Homophonic ciphers
  - Substitute one character for another character
- **Polygram ciphers**
  - substitute a group of characters for another group of characters
  - Goal: make it difficult for frequency analysis

- Invented by Charles Wheatstone
- Named after Lord Playfair
- Used in World War I

Playfair Cipher

- Key table: all the letters into a 5 by 5 table
  - Treat I and J as one, or eliminate Q

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

- Write the keyword (w/o duplicate)at the beginning
  - Key: superbowl

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

Playfair Cipher

- Encryption
  - Divide plaintext into pairs
  - Double characters separated by dummy character (x)
  - mi ss is si pp i becomes mi sx si sx si px pi
  - If plaintext has odd number of chars, append dummy char.
- Encrypt plaintext pair-by-pair using the keybook.

Playfair Cipher

- A pair of plaintext characters could be:
  - same row in the key table
  - same column
  - different row and column
- Same row
  - Substitute with letters on the right
  - mi → nk

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

Playfair Cipher

- Same row
  - Substitute with letters on the right
  - mi → nk
- Same column
  - Substitute with letters below
  - si → bt

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

Playfair Cipher

- Same row
  - Substitute with letters on the right
  - mi → nk
- Same column
  - Substitute with letters below
  - si → bt
- Different column and row
  - substitute plaintext letter with letter that is in its own row, and is in the column of the other plaintext letter
  - sx → pt

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

Playfair Cipher

- Example
  - K = superbowl
  - P = misxsisxsipxpi
  - C = nkptbtptbtwpsm
- Practice:
  - K = superbowl
  - P = rock chalk jayhawk

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

Playfair Cipher

- Example
  - K = superbowl
  - P = misxsisxsipxpi
  - C = nkptbtptbtwpsm
- Practice:
  - K = superbowl
  - P = rock chalk jayhawk
  - C = uadidcbamklzqhom

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

Substitution cipher

- Substitution ciphers
  - Monoalphabetic cipher
  - Polyalphabetic ciphers
  - Homophonic ciphers
  - Polygram ciphers
  - "classical ciphers"
- Still vulnerable to various attacks
  - Brute force attack ➔ when key space is small
  - How to generate a large keyspace?

Substitution cipher

- Vigenere Cipher (and other substitution ciphers) suffers from short keys
  - Brute force attack
- What if we can use a very, very long key?
- One-time pad (Vernam Cipher)
  - Gilbert Vernam (AT&T): 1917
  - Take a stream of random data (keystream)
  - Use it as the key to encrypt the plaintext
  - Message receiver uses same keystream to recover plaintext

One-time pad

- If the stream is truly random → perfect security!
  - Proven to be impossible to crack!
- How to encrypt?
  - Bit-wise XOR
  - Shift (plaintext + key mod 26)

One-time pad

- Bit-wise XOR
- First, XOR (Exclusive or) as a logic operator

A	B	A XOR B
FALSE	FALSE	FALSE
FALSE	TRUE	TRUE
TRUE	FALSE	TRUE
TRUE	TRUE	FALSE

- Also known as: A != B

One-time pad

- Bit-wise XOR
- "Modulo-2"

A	B	A⊕B
0	0	0
0	1	1
1	0	1
1	1	0

One-time pad

- Bit-wise XOR

A	B	A⊕B
0	0	0
0	1	1
1	0	1
1	1	0

$$k \oplus k = 0$$

$$p \oplus k \oplus k = p$$

加密解密==本身

One-time pad

- Bit-wise XOR
  - Encryption: plaintext XOR keystream
  - Example: plaintext = “Cafe”

c:	C	a	f	e
binary:	01000011	01100001	01100110	01100101
key:	33	72	31	79
binary:	00100001	01001000	00011111	01001111
c ⊕ k:	01100010	00101001	01111001	00101010

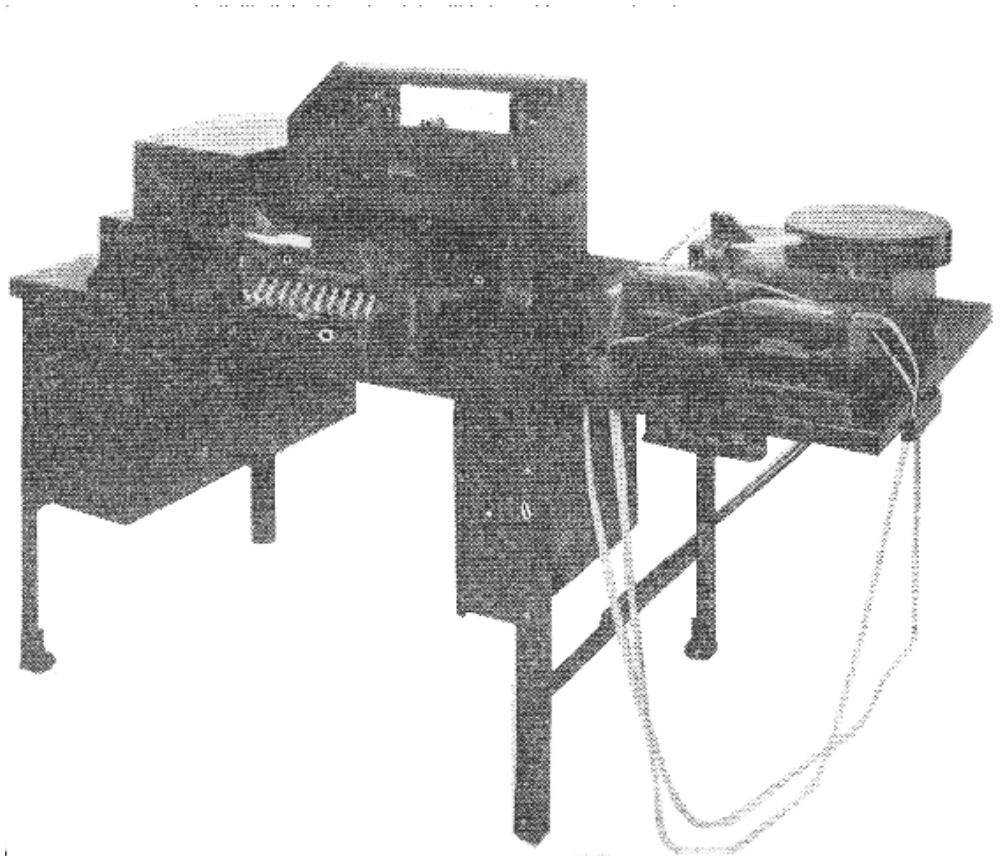
One-time pad

- Bit-wise XOR
  - Decryption: ciphertext XOR keystream
  - Example: plaintext = “Cafe”

c:	C	a	f	e
binary:	01000011	01100001	01100110	01100101
key:	33	72	31	79
binary:	00100001	01001000	00011111	01001111
p ⊕ k:	01100010	00101001	01111001	00101010
key:	33	72	31	79
binary:	00100001	01001000	00011111	01001111
c ⊕ k:	01000011	01100001	01100110	01100101

One-time pad

- Vernam's Cipher Machine
  - Three tapes: plaintext, key, ciphertext



One-time pad

- Shift
  - Vigenere cipher with a very long key
  - plaintext + key mod 26
  - When the plaintext and keystream are both letters-only

One-time pad

- Poorman's one-time pad
- "Book ciphers"
  - Alice and Bob share a book as key
  - novels
  - newspapers
  - telephone books
  - pieces of music
  - decks of cards

Rotor machines

- Implements a kind of Vigenere tableau
- Rotor machines:
  - Keypad (to input plaintext)
  - Several rotors (to generate keys)
  - Keypad wired to a rotor and rotors wired to each other

Rotor machines

- Operation:
  - After each key is pressed, at least one rotor spins (gets a new mapping)
  - An output is generated for the pressed key
  - Rotors positions don't repeat until $26^{\#rotors}$ keys have been pressed
- Effect: $26^{\#rotors}$ substitution alphabets
- Sender and receiver agree on an initial state of the rotors (key).
- Most rotor machines are designed to be involution: encrypt the ciphertext with the same initial settings generates the plaintext.
- Most famous rotor machine: Enigma

Rotor machines

- Most famous rotor machine: Enigma

Rotor machines

- Rotor machines
- A very important part of history
  - 1920s to 1970s
  - not just history of cryptography!
- The ideas are used in DES

Transposition Ciphers

- We have covered substitution ciphers
- Another major topic in classical cryptography
- Rearrange the plaintext to get ciphertext
- Example:
  - P = BOREDOM
  - C = MOODERB
- Q: what is the most important issue in transposition ciphers?

Columnar Transposition

- Use a two-dimensional array (*matrix*)
  - Write plaintext in rows
  - Read ciphertext in columns
- Example
  - P = “ROCKCHALKJAYHAWK”

1	**2**	**3**	**4**	**5**
R	O	C	K	C
H	A	L	K	J
A	Y	H	A	W
K				

Columnar Transposition

- Use a two-dimensional array (*matrix*)
  - Write plaintext in rows
  - Read ciphertext in columns
- Example
  - P = "ROCKCHALKJAYHAWK"

1	**2**	**3**	**4**	**5**
R	O	C	K	C
H	A	L	K	J
A	Y	H	A	W
K				

- Ciphertext: RHAKOAYCLHKKACJW

Columnar Transposition

- Use a two-dimensional array (*matrix*)
  - Write plaintext in rows
  - Read ciphertext in columns
- Example
  - P = "ROCKCHALKJAYHAWK"

1	**2**	**3**	**4**	**5**
R	O	C	K	C
H	A	L	K	J
A	Y	H	A	W
K				

- Could reorder columns: CLHOAYCJWKKARHAK

General Transposition

- Most transpositions use fixed period d
- Let Z_d be the integers from 1 to d
- Let f: $Z_d \rightarrow Z_d$ be a permutation over Z_d
- Key for the cipher is K = (d, f)
- Message:

  $M = m_1, m_2, ..., m_d, m_{d+1}, ..., m_{2d}, ...$
- Ciphertext

  $C = m_{f(1)}, m_{f(2)}, ..., m_{f(d)}, m_{d+f(1)}, ..., m_{d+f(d)}, ...$

General Transposition

- Example:
  - suppose that the period $d = 4$
  - suppose that f is:

i	1	2	3	4
$f(i)$	2	4	1	3

  - P = ROCK CHAL K
  - C = OKRC HLCA K
  - Last block: K␣ ␣ ␣ → ␣ ␣K␣

General Transposition

- Cryptanalysis
  - First, how to determine if it is a transposition cipher?
  - Break the transposition cipher
  - Use common letter pairs (digrams), triples (trigrams) to figure out *d*

Combinations of Approaches

- It is not too difficult to break basic substitutions and basic permutations
- Use a combination of the two → **product cipher**
  - Substitution adds **confusion**
  - Transposition adds **diffusion**

替代是破译变得更混乱；
交换使破译答案变得更离散

Combinations of Approaches

- Confusion and Diffusion
  - Claude Shannon ("father of information theory"): *Communication Theory of Secrecy Systems*, 1949.
  - Shannon Secrecy

    $P(M = m \mid E(K, m) = c) = P(M = m)$

    - Probability of guessing the plaintext knowing the ciphertext = probability of guessing plaintext without knowing ciphertext.

    $P(E(K, m) = c) = P(E(K, m') = c)$

    - Probability of any message giving a ciphertext is the same

Combinations of Approaches

- Confusion and Diffusion
  - Confusion: make the relationship between the plaintext and the ciphertext (or the ciphertext and the key) as complex as possible.
    - Use the key in a very complex way.
  - Diffusion: dissipate the statistical structure of the plaintext in the long range statistics of the ciphertext.
    - Have many plaintext characters (bits) affect each ciphertext character (bit)

Combinations of Approaches

- Confusion and Diffusion
  - Claude Shannon introduced idea of *substitution-permutation (S-P)* networks (1949)
  - The basis of modern block ciphers
  - S-P networks are based on the two primitive cryptographic operations:
    - substitution (**S-box**)
    - permutation (**P-box**)
    - we will see them in DES (1974)
  - Provide **confusion** and **diffusion** of message

Stream and Block Ciphers

- Stream ciphers
  - encrypt one symbol (bit, letter) at a time
  - encrypt the i^{th} symbol with the i^{th} part of the keystream
- Block ciphers
  - Encrypt larger blocks of plaintext
  - Encrypt all blocks with the same key
  - E.g. the transposition cipher example:
    - Encrypt 4 letters at once
    - Cannot just encrypt letter 1 – need to wait for the other letters in the block.

Stream and Block Ciphers

- Stream ciphers
  - Vernam (one time pad)
  - Vigenere with period p
  - Rotor machine with r rotors: period of 26^r
- Block ciphers
  - Transposition ciphers with period p
  - Playfair

Stream and Block Ciphers

- Stream ciphers
  - Advantages: fast; low error propagation
  - Disadvantages: low diffusion; vulnerable to insertions and modifications
- Block ciphers
  - Advantages: high diffusion; more immunity to insertion
  - Disadvantages: slower; error propagation

Summary

- So far, we have learned
  - Terminology
  - Cryptography and Cryptanalysis
  - Secret key Cryptography
    - Substitution ciphers
      - Caesar, Shift, Vigenere, Homophonic, Playfair
      - One-time pad, rotor machines
    - Transposition ciphers
    - Combinations
    - Shannon's theory of secrecy systems