BitsAndBytes2017: Cryptography

Some terminology

Plaintext
Ciphertext

Encrypt (encryption)
Decrypt (decryption)

Bob and Alice (and "Bad Guy")

Why use cryptography?

What kinds of things need to be kept secret?

- Money and war – the two biggies in human history.
- Passwords
- Intellectual property
- Embarrassing information
- Geographical location
- etc.

TapCode

	1	2	3	4	5
1	A	B	C/K	D	E
2	F	G	H	I	J
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Example:

M	I	C	H	I	G	A	N
(3, 2)	(2, 4)	(1, 3)	(2, 3)	(2, 4)	(2, 2)	(1, 1)	(3, 3)
••• ••	•• ••••	• •••	•• •••	•• ••••	•• ••	• •	••• •••

To encrypt:
Look up letter in the table.
Tap row numbers, followed by column number

To decrypt:
Read off the letter (row is # of taps, then column is # taps)

Steganography – "Hidden Writing"

Many techniques:

- Invisible ink
- Pin pricks over words
- Skipping words, e.g., message is every 4th word
- Hide message in digital text or digital pixels, using unimportant bits.
- Et cetera

Example: Using pinpricks "gold under dog house"

Dear Mother,

All is well here, though I often think of autumn at home in Colorado: the gold aspen leaves, the crisp air. I have been a bit under the weather, but I am not sick as a dog. I hope the roof on our house stays tight until I can get home.

Your son, Goose

Example: using every 5th word "GOLD UNDER DOG HOUSE"

Dear Mother,

Is the gold cat OK? He hides under the sofa. My old dog needs a warmer, drier house.

Your son, Goose

Read off the letter (row is # of taps, then column is # taps)

ShiftCipher

Secret key: the amount of shift

To Encrypt:

Look up letter
Move to the right shift steps, wrap-around if needed

To Decrypt:

Look up the letter
Move to the left shift steps, wrap-around if needed

Example

Key = 3 (also known as Caesar cipher, named for Julius Caesar, emperor of Rome)

M	I	C	H	I	G	A	N
P	L	F	K	L	J	D	Q

Vigenère Cipher

Notice that when you give the key for a Caesar cipher, you could give the number, or you could give the letter.

For example:

a shift of 3 can be specified with "D"
a shift of 10 can be specified with "K"

Try it. Using a shift of "D", decrypt

J R Q H R X W

The Vigenere Cipher uses a key that is a word. Each letter in the word specifies the shift to be used on the current plaintext (for encryption) letter.

Example: Suppose the key is "doggie". Notice the key repeats as needed.

To encrypt	I	L	I	K	E	C	A	T	S
Use the key	D	O	G	G	I	E	D	O	G
The cipher text is:	L	O	O	Q	M	G	D	H	Y

General Substitution Cipher

The secret key is the entire alphabet, jumbled.

Example

Original order:
|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|

Jumbled order:
|Z|Y|X|W|A|B|C|D|V|U|T|E|F|G|H|I|J|K|T|S|R|J|K|L|M|N|

Plaintext: HERE COMES THE SUN
Ciphertext: DAKA XHFAT SDA TRG

Transposition (Permutation)

Secret key: Rearrangement order.

Example: Secret key is 5 3 1 4 2

- Write plaintext in groups of 5 characters, no blanks, append with X or Q as needed.
- Letters in a group of five gets numbered 1 – 5.
- Rearrange the numbers using the secret key:

Original plaintext: `HERE COMES THE SUN`

Groups of 5 with numbers:
```
HEREC OMEST HESUN
12345 12345 12345
```
Rearranged: `CRHEE TEOSM NSHUE`

Example: secret key is 4 3 1 2

Original plaintext: `DETROIT MICHIGAN`

Groups of 4:
```
DETR OITM ICHI GANX
1234 1234 1234 1234
```

Ciphertext; `RTDE MTOI IHIC XNGA`

Cryptanalysis

Use frequency of letters

Top 12 most common letters in English:

E	12.7%
T	9.1%
A	8.2%
O	7.5%
I	7.0%
N	6.7%
S	6.3%
H	6.1%
R	6.0%
D	4.3%
L	4.0%
U	2.8%

Top 5 most common first letter of an English word:

T	16.7
A	11.6
S	7.6
H	7.3
W	6.8

Consider this cipher text – count the most commonly appearing letters.

```
TDZL JLI PHRLJFO UCM ZLLY MKL VBF
```

counts: L: 6, F: 2, J: 2, M: 2

Try L→ E `TDZe JeI PHReJFO UCM ZeeY MKe VBF`

Try M → T `TDZe JeI PHReJFO UCt ZeeY tKe VBF`

Continue with the most likely trials, backtracking when you detect failure (this is called "hypothesize and test", a famous algorithm in AI)

The plaintext -> `MAKE NEW FRIENDS BUT KEEP THE OLD`

Using brute force to break ciphers

Guess an encryption algorithm, try all possible keys.

EXAMPLE: Guess shift cipher, try all shift sizes

Ciphertext: `WZBDI VO OCZ WZBDIIDIB`

```
K=18:      . . .
K=19:     ZCEGL YR RFC ZCEGLLGLE
K=20:     ADFHM ZS SGD ADFHMMHMF
K=21:     BEGIN AT THE BEGINNING   ← the plaintext
K=22:     CFHJO BU UIF CFHJOOJOH
K=23:     . . .
```

Public Key

All messages to Alice should be encrypted (maybe Alice is a credit card company).

Alice creates a linked set of keys using a special mathematical property of prime numbers: (K, P)

one is made public, K
the other is kept private P.

Bob wants to send an encrypted message to Alice.

(1) He looks up Alice's public key, K
(2) Bob encrypts his plaintext with K (using arithmetic)
(3) Bob sends the ciphertext to Alice.

Alice receives the ciphertext.

Alice uses her private key, P, to decrypt the ciphertext to plaintext (using arithmethic).

Can Bob figure out Alice's Private key? Computers are not powerful enough … yet.
Can Bob decrypt his own ciphertext? NO! Bob can't convert from cipher text to plaintext
What can a Bad Guy see?

He can see Alice's public key K
He can see Bob's encrypted message

What are Bad Guy's options?

Steal Alice's Private key from Alice
Steal Bob's plaintext from Bob.

Secret Key versus Public Key

Both Bob and Alice need to know Secret Key
Advantage Public Key
How do they exchange that secret?

Modern Secret Key works with substitution
Advantage Public Key
and transposition: more vulnerable to
code-breaking

Anyone can send a Public Key encrypted message
Advantage Public Key
to Alice, not just the ones who know the secret

For equivalent levels of strength against code-breaking,
Advantage Secret Key
Secret Key is faster to encrypt/decrypt
than Public Key.

PLAYFAIR

Secret key is a word or phrase. Use it to construct the Playfair square:

Example: EASTERN MICHIGAN UNIVERSITY. Use each letter only once. Fill in the rest of the square with the remainder of the alphabet in order. I and J occupy the same space. EAST~~E~~RN MICH~~I~~G~~AN~~ U~~NI~~V~~ERSIT~~Y

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

LITTLE DOGGY PET → LI TX TL ED OG GY PE TX KC CT CX NP DB UB EN CT

To encrypt:

(1) Group plaintext into two letter pairs; for any duplicate letters in a pair, insert X.

(2) Find pair of letters on square, using wrap-around.

If letters are corners of a box, output the other corners (row letter, then column letter)

If letters are on same row, output letters one step to the right

If letters are on same column, output letters one step down.

Sliders for shifting

0	A	0	A
1	B	1	B
2	C	2	C
3	D	3	D
4	E	4	E
5	F	5	F
6	G	6	G
7	H	7	H
8	I	8	I
9	J	9	J
10	K	10	K
11	L	11	L
12	M	12	M
13	N	13	N
14	O	14	O
15	P	15	P
16	Q	16	Q
17	R	17	R
18	S	18	S
19	T	19	T
20	U	20	U
21	V	21	V
22	W	22	W
23	X	23	X
24	Y	24	Y
25	Z	25	Z