Lecture Notes

Advanced Discrete Structures

COT 4115.001 S15

2015-01-14

Recap

- Extended Euclidean Algorithm
- Solving $ax + by = d$
- Arithmetic Modulo n
- Finding $a^{-1} \pmod{n}$

Chapter 2

CLASSICAL CRYPTOSYSTEMS

Conventions

- *plaintext* will be written in lowercase
- *CIPHERTEXT* will be written in uppercase
- Letters of the alphabet are assigned numbers:

a	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**
0	1	2	3	4	5	6	7	8	9
k	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**s**	**t**
10	11	12	13	14	15	16	17	18	19
u	**v**	**w**	**x**	**y**	**z**				
20	21	22	23	24	25				

What to do about spaces?

- Spaces are frequent
  - They reveal information about word structure
  - If spaces encrypted, easy to identify by frequency giving the ability to crack key.

Classical Cryptosystems - Section 2.1

SHIFT CIPHERS

Shift ``Caesar" Cipher (~45BC)

Example: Shift each letter to the right by three.

Original:

`gaul is divided into three parts`

By Convention: `gaulisdividedintothreeparts`

Shifted by 3: `JDXOLVGLYLGHGLQWRWKUHHSDUWV`

Mathematically:

$$x \longmapsto x + \kappa \pmod{26}$$

Encryption

$$x \longmapsto x - \kappa \pmod{26}$$

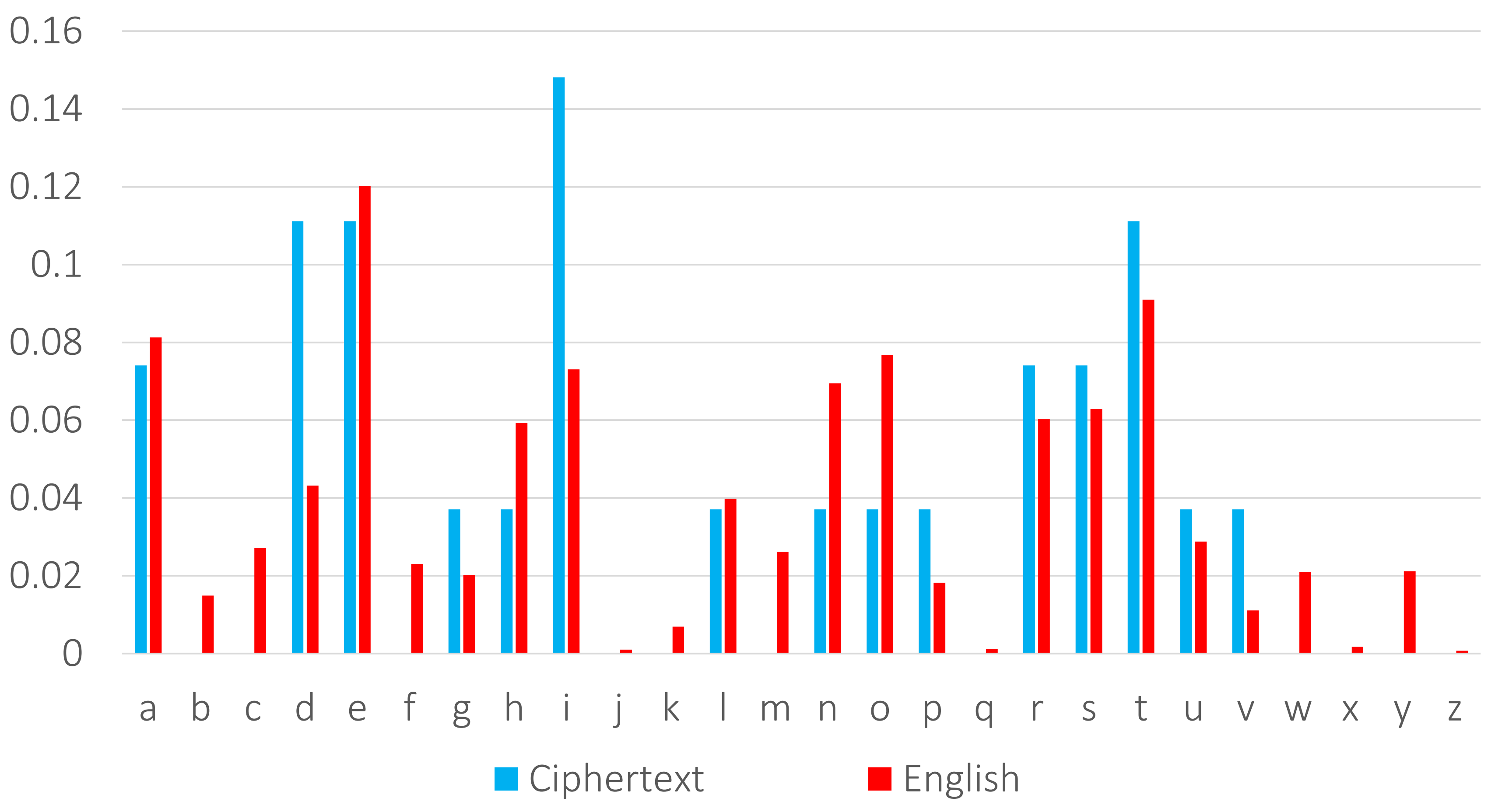
Decryption

Attacks on Shift Cipher

1. **Ciphertext Only:**
   - Brute force it!
   - Frequency analysis

```
0:  gaulisdividedintothreeparts
1:  hbvmjtejwjefejoupuisffqbsut
2:  icwnkufkxkfgfkpvqvjtggrctvu
3:  jdxolvglylghglqwrwkuhhsduwv
4:  keypmwhmzmhihmrxsxlviitevxw
5:  lfzqnxinanijinsytymwjjufwyx
6:  mgaroyjobojkjotzuznxkkvgxzy
7:  nhbspzkpcpklkpuavaoyllwhyaz
8:  oictqalqdqlmlqvbwbpzmmxizba
9:  pjdurbmrermnmrwcxcqannyjacb
10: qkevscnsfsnonsxdydrboozkbdc
11: rlfwtdotgtopotyezescppalced
12: smgxuepuhupqpuzfaftdqqbmdfe
13: tnhyvfqvivqrqvagbguerrcnegf
14: uoizwgrwjwrsrwbhchvfssdofhg
15: vpjaxhsxkxstsxcidiwgttepgih
16: wqkbyitylytutydjejxhuufqhji
17: xrlczjuzmzuvuzekfkyivvgrikj
18: ysmdakvanavwvaflglzjwwhsjlk
19: ztneblwbobwxwbgmhmakxxitkml
20: auofcmxcpcxyxchninblyyjulnm
21: bvpgdnydqdyzydiojocmzzkvmon
22: cwqheozerezazejpkpdnaalwnpo
23: dxrifpafsfabafkqlqeobbmxoqp
24: eysjgqbgtgbcbglrmrfpccnyprq
25: fztkhrchuhcdchmsnsgqddozqsr
```

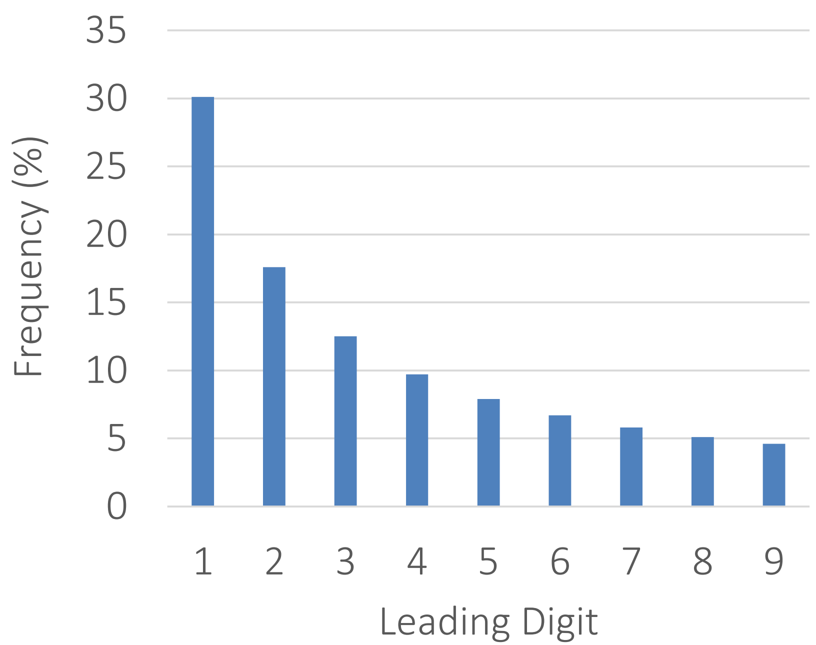
English Language (Frequency Analysis)



Benford's Law

- **Benford's Law**, also called the **First-Digit Law**, refers to the frequency distribution in many (but not all) real-life sources of data.

Leading Digit	Occurring Frequency
1	30.1%
2	17.6%
3	12.5%
4	9.7%
5	7.9%
6	6.7%
7	5.8%
8	5.1%
9	4.6%



Attacks on Shift Cipher

2. Known plaintext:

- If you know one letter, you can decipher the rest

Example:

d $(= 23) \longmapsto$ N $(= 13)$, $\kappa \equiv 13 - 23 \equiv -10 \equiv 16 \pmod{26}$

3. Chosen plaintext:

- Encrypt the letter a and compute the difference.

4. Chosen ciphertext:

- Decrypt the letter A and compute the difference.

Classical Cryptosystems - Section 2.2

AFFINE CIPHERS

Affine Ciphers

Shift Cipher:

$$x \longmapsto x + \kappa \pmod{26}$$

for some $\kappa \in \mathbb{Z}$.

Affine Cipher:

$$x \longmapsto \alpha\, x + \beta \pmod{26}$$

for some $\alpha, \beta \in \mathbb{Z}$ with $\gcd(\alpha, 26) = 1$.

Affine Ciphers

Example: $\alpha = 3, \;\; \beta = 5$ (Check: $\gcd(3,26) = 1$ ✓)

	m	a	t	h	i	s	f	u	n	
	12	0	19	7	8	18	5	20	13	
x3	10	0	5	21	24	2	15	8	13	(mod 26)
+5	15	5	10	0	3	7	20	13	18	
	P	F	K	A	D	H	U	N	S	

$$3x + 5 \equiv X \pmod{26}$$

$$x \equiv 3^{-1}(X - 5) \pmod{26} \qquad 3^{-1} \equiv 9 \pmod{26}$$

$$x \equiv 9\,X + 7 \pmod{26}$$

Affine Ciphers

Example: $x \equiv 9\,X + 7 \pmod{26}$

	m	**a**	**t**	**h**	**i**	**s**	**f**	**u**	**n**	
	12	0	19	7	8	18	5	20	13	
x3	10	0	5	21	24	2	15	8	13	(mod 26)
+5	15	5	10	0	3	7	20	13	18	
	P	**F**	**K**	**A**	**D**	**H**	**U**	**N**	**S**	
	15	5	10	0	3	7	20	13	18	
x9	5	19	12	0	1	11	24	13	6	(mod 26)
+7	12	0	19	7	8	18	5	20	13	
	m	**a**	**t**	**h**	**i**	**s**	**f**	**u**	**n**	

<u>Encryption Key</u>: $(\alpha, \beta) = (3,5)$ <u>Decryption Key</u>: $(\alpha', \beta') = (9,7)$

Affine Ciphers

What can happen if $\gcd(\alpha, 26) > 1$?

Example:

$x \longmapsto 13x + 4$ $\quad$ `input` $\longmapsto$ ERRER

$\gcd(13,26) = 13$ $\quad$ `alter` $\longmapsto$ ERRER

How many possible pairs (α, β) with $\gcd(\alpha, 26) = 1$?

- $2 \mid \gcd(2k, 26)$ leaves 13 odd numbers
- $13 \mid \gcd(13k, 26)$ leaves 12 possibilities for α
- $12 \times 26 = \mathbf{312}$ choices for the key (α, β)

Attacks on Affine Ciphers

1. **Ciphertext only:**
   - Brute force all 312 keys!
   - Frequency Analysis
2. **Known plaintext:**
   - Knowing two letters allows you to find the key:

$$X \equiv \alpha\, x + \beta \pmod{26} \qquad \text{and} \qquad Y \equiv \alpha\, y + \beta \pmod{26}$$

$$\alpha\,(x - y) \equiv X - Y \pmod{26}$$

If $\gcd(x - y, 26) = d > 1$, then $d \mid X - Y$ first divide both $x - y$ and $X - Y$ by d. Then:

$$\alpha \equiv (X - Y)(x - y)^{-1} \pmod{26}$$

$$\beta \equiv X - \alpha\, x \pmod{26}$$

Attacks on Affine Ciphers

Example: $\texttt{c} \longmapsto \texttt{Z}$ and $\texttt{e} \longmapsto \texttt{M}$

$2 \longmapsto 25$ $\quad$ $15 \longmapsto 12$

$$25 \equiv 2\alpha + \beta \pmod{26} \quad \text{and} \quad 12 \equiv 15\alpha + \beta \pmod{26}$$

$$13 \equiv -13\alpha \pmod{26}$$

- No multiplicative inverse, $(-13)^{-1}$, modulo n.
- Note that: $\gcd(-13, 26) = 13$.
- Divide both sides by 13 and solve:

$$1 \equiv -1 \cdot \alpha \pmod{26} \quad \text{and} \quad (-1)^{-1} \equiv -1 \pmod{26}$$

$$\alpha \equiv -1 \cdot -1 \equiv 1 \pmod{26}$$

$$\beta \equiv 25 - 2 \cdot 1 \equiv 23 \pmod{26}$$

- Check:

$$25 \equiv 2 \cdot 1 + 23 \pmod{26} \quad \text{and} \quad 12 \equiv 15 \cdot 1 + 23 \pmod{26} \ \checkmark$$

Attacks on Affine Ciphers

Chosen plaintext:

- Choose `ab (=01)` as the plaintext. This gives:

$$X \equiv \alpha \cdot 0 + \beta = \beta \pmod{26} \quad \Longrightarrow \quad \beta \equiv X \pmod{26}$$
$$Y \equiv \alpha \cdot 1 + \beta \pmod{26} \quad \Longrightarrow \quad \alpha \equiv Y - \beta \equiv Y - X \pmod{26}$$

<u>Encryption</u>: $(Y - X,\ X)$ <u>Decryption</u>: $((Y-X)^{-1}, -(Y-X)^{-1}X)$

Chosen ciphertext:

- Choose `AB (=01)` as the ciphertext. This gives:

$$0 \equiv \alpha \cdot x + \beta \pmod{26}$$
$$1 \equiv \alpha \cdot y + \beta \equiv \alpha\,(y - x) \pmod{26} \quad \Longrightarrow \quad \alpha \equiv (y-x)^{-1} \pmod{26}$$
$$\beta \equiv -\alpha \cdot x \equiv -(y-x)^{-1}x \pmod{26}$$

<u>Encryption</u>: $((y-x)^{-1}, -(y-x)^{-1}x)$ <u>Decryption</u>: $(y - x,\ x)$

Classical Cryptosystems - Section 2.3

THE VIGENÈRE CIPHER

Vigenère Cipher Encryption

1. Choose a random key:

```
key: bacon
```

2. Match message to key repeats:

```
plaintext: whatdoesthefoxsay
      key: baconbaconbaconba
```

3. Add message and key to get ciphertext

Vigenère Cipher En(De)cryption

w	h	a	t	d	o	e	s	t	h	e	f	o	x	s	a	y
22	7	0	19	3	14	4	18	19	7	4	5	14	23	18	0	24
+																
b	a	c	o	n	b	a	c	o	n	b	a	c	o	n	b	a
1	0	2	14	13	1	0	2	14	13	1	0	2	14	13	1	0
23	7	2	7	16	15	4	20	7	20	5	5	16	11	5	1	24
X	**H**	**C**	**H**	**Q**	**P**	**E**	**U**	**H**	**U**	**F**	**F**	**Q**	**L**	**F**	**B**	**Y**

To decrypt, subtract key in the say fashion.

Attacks on the Vigenère Cipher

- <u>Plaintext attack</u>
  - If enough characters are known, the key is obtained.
- <u>Chosen plaintext</u>
  - Choose the plaintext: `aaaa`… . Ciphertext is the key
- <u>Chosen ciphertext</u>
  - Choose the ciphertext `AAAA`… . Plaintext is negative of the key

Attacks on the Vigenère Cipher

- <u>Ciphertext only</u>
  - Does frequency analysis work?
    - In the example, `e` can become either `F`, `E`, `G`, `S`, or `R`
    - Letter frequencies become "averaged"
  - Can we guess the length of the key?
    - Try displacing the message and counting the coincidences, when a letter matches the displaced letter
  - If we can guess the key length, perhaps we can recover the letter frequency and recover the key

Classical Cryptosystems - Section 2.3.1

FINDING KEY LENGTH

Attacks on the Vigenère Cipher

- **Example:**

```
plain:  whatdoesthefoxsay
cipher: XHCHQPEUHUFFQLFBY
```

d=1	XHCHQPEUHU**F**FQLFBY	1
d=2	X**H**CHQPE**U**HUFFQLFBY	2
d=3	XHCHQPEUHUF**F**QLFBY	1
d=4	XHCHQPEUHU**F**FQLFBY	1
d=5	XHC**H**QPEUHUFFQLFBY	1

Message is too short!

English Language (Frequency Analysis)