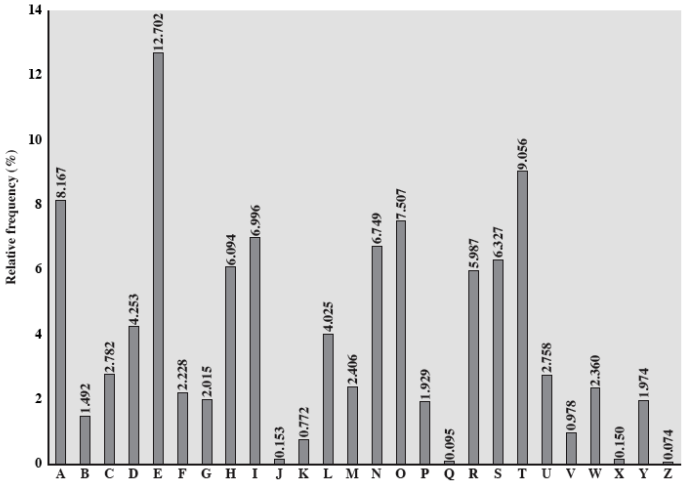
Welcome to Bletchley Park

Playfair and Enigma

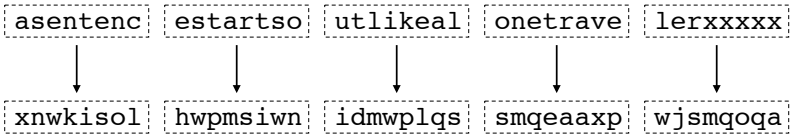
CS310 Cryptography

Department of Computer Science
Wellesley College

Substitution falls prey to frequency analysis

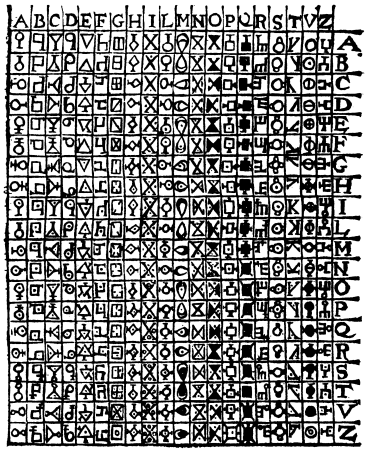


Polygraphic substitution



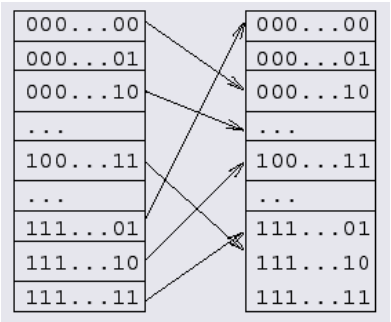
Graphemes

- Digraphic substitutions ($V^2 \rightarrow W^m$) quite common.
- One of the oldest polygraphic encryptions of this type is found in Giovanni Battista Porta's *De furtivis literarum notis* (1563).

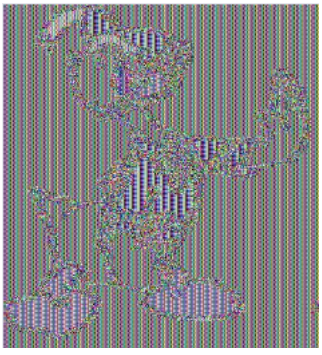


Block ciphers

- Modern block ciphers substitute one bit string of length *n* (block size) for another.
- For example, 3DES uses a block size of 64.
- For the English language this is probably too large a block size to give useful variations in frequencies.

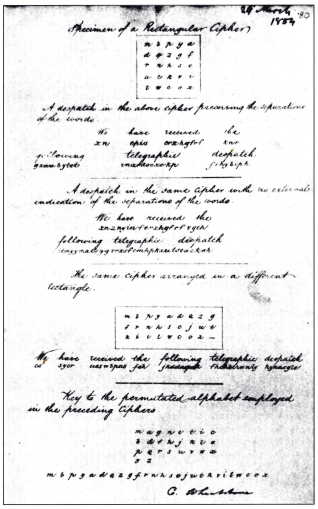


However, for image encryption ...

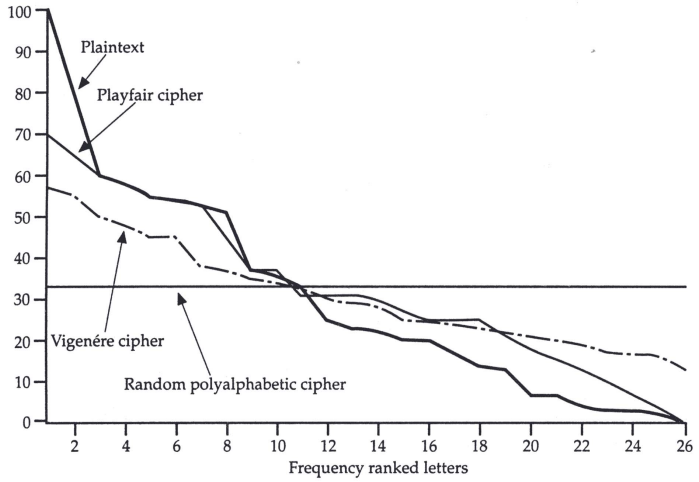


Playfair cipher

- In 1854, Charles Wheatstone invented a special bipartite digraphic subsititution.
- His friend, Lyon Playfair, Baron of St. Andrews recommended to the government and it pressed into service for the Crimean and Boer Wars.
- Used by the British in WW I, it was routinely broken by the Germans.



Relative frequencies of letters



Lord Peter & Ms. Vane solve a mystery

- The Playfair is based on the use of 5 x 5 matrix of letters constructed using a keyword.
- Lord Peter Wimsey explains in Dorothy Sayers' s *Have His Carcase.*

Donut rules

- If the two letters are not in the same row or column, replace each letter by the letter that is in its row, and is in the column of the other letter.
- If the two letters are in the same row, replace each letter with the letter immediately to its right.
- If the two letters are in the same column, replace each letter with the letter immediately below it.

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

meet at the schoolhouse
        ↓
me et at th es ch ox ol ho us ex
        ↓
EG MN FQ QM KN BK SV VR GQ XN KU
```

Cryptoanalysis

HR KY LD ZX NQ EO ND EC TC TI AD CT AK RH LB GT SN AN

UN ON DR HX PE BN ZC DT KV EQ HD AO HR DU RP TQ OB DE

QD HR KY YA HZ HB BU KZ EQ XG TI BI KY RI CQ HR CE CO

SX RM BC TH CG QD RK NQ IT DC WT FV UB YA GU HE CZ NU

LB IQ YK FV UB IQ WD QB UN KM DE TD KA HR NU OU

Cryptoanalysis

HR KY LD ZX NQ EO ND EC TC TI AD CT AK RH LB GT SN AN

UN ON DR HX PE BN ZC DT KV EQ HD AO HR DU RP TQ OB DE

QD HR KY YA HZ HB BU KZ EQ XG TI BI KY RI CQ HR CE CO

SX RM BC TH CG QD RK NQ IT DC WT FV UB YA GU HE CZ NU

LB IQ YK FV UB IQ WD QB UN KM DE TD KA HR NU OU

Possible relationships

- We have two equations:

  HR=th and *KY=is*

- Since the first has only three letters, one of the linear arrangements must have been used, and the common letter, *H*, must have stood between the other two.
- Possible three letter arrangements

Vertical	Horizontal
T	
H	T H R
R	

The other equation *KY=is*

- ... the positions of the letters are not so definite. In a linear arrangement, *IK* and *SY* must be in direct sequence, although either sequence may come first.

Vertical	Horizontal	Rectangular
I		
K		I * K
*	I K * S Y	* *
S		Y * S
Y		

We suspect the presence *"condemation"*

- Slide the word *"condemation"* across the text. Many positions are impossible, since in Playfair no letter may be its own substitute:

```
HR KY LD ZX NQ EO ND EC TC TI AD CT AK RH LB GT SN AN
               co nd em na ti on
```

- The next position is more promising:

```
HR KY LD ZX NQ EO ND EC TC TI AD CT AK RH LB GT SN AN
               *c on de mn at io n*
```


Possible relationships

- Implications of the first two equations

```
HR KY LD ZX NQ EO ND EC TC TI AD CT AK RH LB GT SN AN
               *c on de mn at io n*

1  2     3  4        5  6     7     8
O        D           O
N  O N D  E  D E C    N  O N D  O
D        C           D     E  N     O N D E C
                     E     C  D E C
                     C
```

Possible relationships: Third equation

- Implications of the first three equations

```
HR KY LD ZX NQ EO ND EC TC TI AD CT AK RH LB GT SN AN
               *c on de mn at io n*
```

```
1  2      3  4        5  6     7  8
O          D          O
N  O N D   E  D E C   N  O N D  O
D          C          D     E  N   O N D E C
                      E     C  D E C
                      C
```

```
9  10           11
M
T              M * T
*  M T * N C   *   *
N              C * N
C
```

```
12
O N D E C
  *     *
  T     M
```

Playfair and Enigma 1-17

Possible relationships: Forth equation

- Implications of the first four equations

```
HR KY LD ZX NQ EO ND EC TC TI AD CT AK RH LB GT SN AN
               *c on de mn at io n*
```

```
12
O N D E C
  *     *
  T     M
```

```
13  14
A
T   A T I
I
```

```
15          16
O N D E C   O N D E C
  *     *     *     *
  A     A T I   M
  T     M
  I
```

Playfair and Enigma 1-18

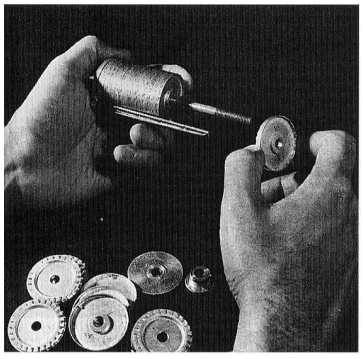
Finishing the cryptogram*

- *Hint:* This same cryptogram contains the word RECONSTRUCT.

*Your first homework assignment.

Mechanization of secrecy

- Advances in cryptanalysis prompted the need for more secure (read more complex) cryptosystems.
- However, the weakest link in any cryptosystem is generally the people who use it.
- Mechanical means promised it all: more complexity with simplicity of use.



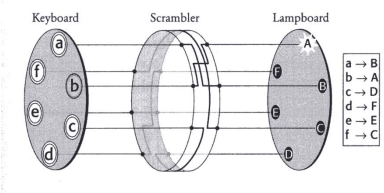
*You get to read all about it in your first assignment.

Cipher disks

- The Confederate Alberti disk may be thought of as a mechanized Caesar cipher.
- However, it can also be used in a manner that is functionally equivalent to the Vigenere cipher.*

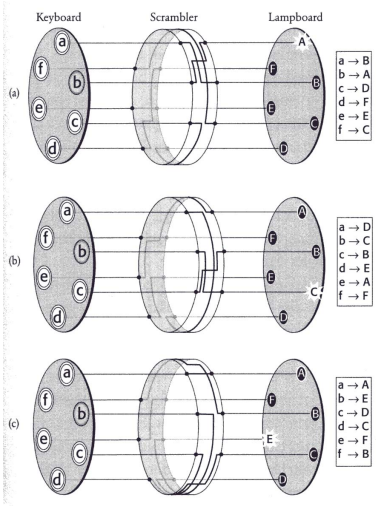
Rotor machines

- Shortly after the first world war, the German firm of Scherbius and Ritter developed an electronic version of the Alberti disk.
- Typing a "b" on the keyboard causes a current to flow through the scrambler and emerge on the other side to illuminate the "a" light lamp.



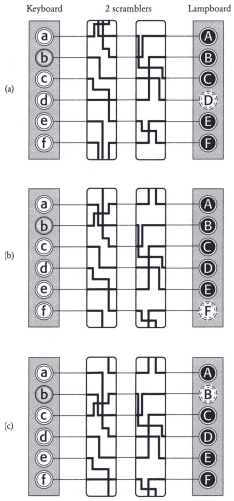
Adding an element of Vigenere

- Every time a letter is typed into the keyboard and encrypted, the scrambler rotates by one place.
- After one rotation, result of typing a "b" is functionally equivalent to first shifting "b" back one position, passing through the scrambler, then shifting the result forward one position.



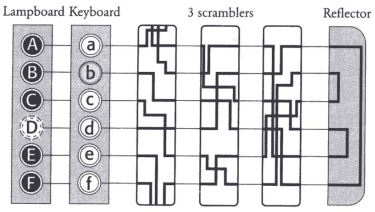
Adding a second scrambler

- With only one scrambler, there are only 26 distinct starting positions.
- This is not a key space that is likely to worry even the dimmest watt bulb.



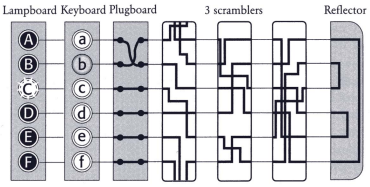
Commercial Enigma machines

- Commercial Enigma machines had three rotors and a reflector.
- The reflector is a *complication illusoire.* But it serves an important role never the less.



Wehrmacht Enigma machines

- The number of keys with three rotors is 26^3 = 17,576.
- A dozen determined cryptographers could search the entire space in a day.
- Early Wehrmacht machines were provided with removable, interchangable rotors and a plugboard.

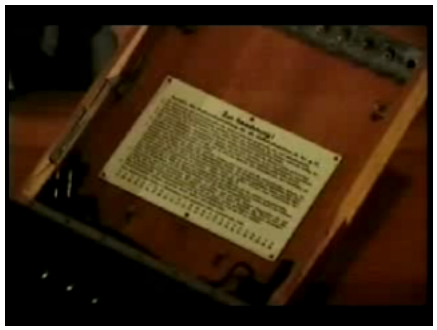


Enigma

- Packaged up and weighing in at about 12 kilos, thousand of Enigmas were distributed throughout the German army by the start of World War II.

Alan Turing meets Enigma

- The best and the brightest were brought to Bletchley Park to break the code.



Alan Turing is helped by the Germans*

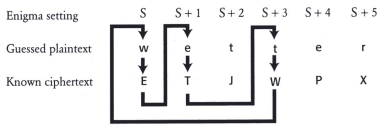
- Turing began by postulating the position of a "crib". In this, he was aided by that fact that no letter ever encipher to itself.
- For example, does the following crib match the given ciphertext?

```
Crib:       w e t t e r n u l l e c h s
CIPHER: I P R E N L W K M J J S X C P E J W Q
```

*By studying old decrypted messages, he believed he could sometimes predict part of the an undeciphered message. For example, Germans sent a regular enciphered weater report shortly after 6 A.M. each day.

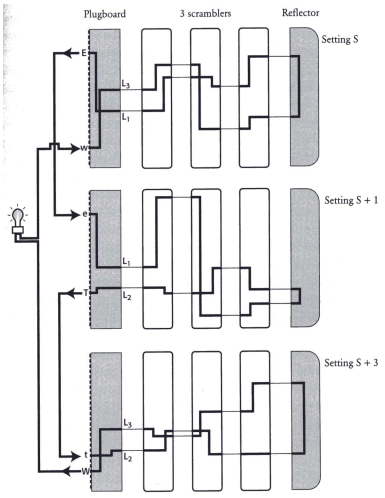
Turing loops

- Next, he constructed a list of internal loops linking plaintext and ciphertext characters.



Turing Bombes

- A consequence of the loop is to nullify the effect of the plugboard.
- Sixty Enigma machines were set up, one for each of the ways of arranging the five rotors taken three at a time.
- These sixty machines clicked around in unison until a circuit was completed and the light illuminated.



Success

- Once the correct scrambler arrangements and orientations had been established, finding the plugboard cabling was a piece of cake.
- By the end of 1942, 49 bombes were clicking around the clock.