Classical Encryption Techniques

Hill Cipher

- Takes m successive plaintext letters and substitutes for them m cipher text letters.
- Uses simple linear equations
- Numbered alphabet: a = 0, b = 1, c = 3, etc.

Hill – key is matrix

$$\begin{matrix} k11 & k12 & k13 \\ k21 & k22 & k23 \\ k31 & k32 & k33 \end{matrix}$$

- Generalize to any size, larger blocks
- Matrix must be invertible

Contd.

- C=(KP)mod 26
- Where C and P are column vectors.
- K is a square matrix (encryption Key)

Strength

- Completely hides single-letter frequencies
- It is strong against a CipherText-only attack

- But.......
- Easily broken with a known PlainText attack

Reduction of a polyalphabetic cipher to a monoalphabetic ciphers

Vigenere Cipher

Vigenère Cipher

- simplest polyalphabetic substitution cipher
- effectively multiple caesar ciphers
- key is multiple letters long $K = k_1\ k_2\ \ldots\ k_d$
- i^{th} letter specifies i^{th} alphabet to use
- use each alphabet in turn
- repeat from start after d letters in message
- decryption simply works in reverse

Example of Vigenère Cipher

- write the plaintext
- write the keyword repeated above it
- use each key letter as a caesar cipher key
- encrypt the corresponding plaintext letter
- eg using keyword *deceptive*

```
key:       deceptivedeceptivedeceptive

plaintext: wearediscoveredsaveyourself

ciphertext:ZICVTWQNGRZGVTWAVZHCQYGLMGJ
```

Security of Vigenère Ciphers

- There are multiple ciphertext letters corresponding to each plaintext letter. So, letter frequencies are obscured.
- To break Vigenere cipher:
  Brute Force Attack……..if key length is known
- If key length is not known

1. Try to guess the key length. How? identify repeated patterns of length of 2 or 3 in the cipher text. Distance between them must be a multiple of the key length. For more repeated segments the GCD of distance will consider as key length.
2. If key length is N, the cipher consists of N Caesar Ciphers. Plaintext letters at positions k, N+k, 2N+k, 3N+k, etc., are encoded by the same cipher.
3. Ex: If GCD is 4, which means that the key length is multiple of 4. Divide the Ciphertext into four pieces. Piece C1 is made of characters 1,5,9….Piece C2 is made of characters 2,6,10….and so on.
4. Use the statistical attack on each individual cipher as before.

Transposition Ciphers

- Also called **permutation** ciphers.
- Shuffle the plaintext, without altering the actual letters used.
- Example: Row / ColumnTransposition Ciphers

Transposition Ciphers

- Plaintext is written row by row in a rectangle.
- Ciphertext: write out the columns in an order specified by a key.

```
Key: 4 3 1 2 5 6 7
```

```
Plaintext:
```

a	t	t	a	c	k	p
o	s	t	p	o	n	e
d	u	n	t	i	l	t
w	o	a	m	x	y	z

```
Ciphertext: TTNAAPTMTSUOAODWCOIXKNLYPETZ
```

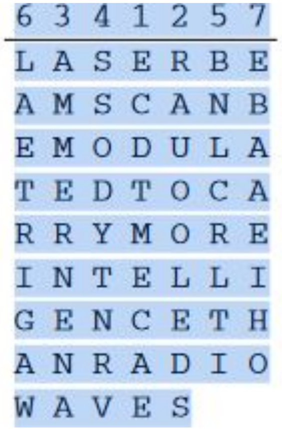
Contd..

Columnar transposition:

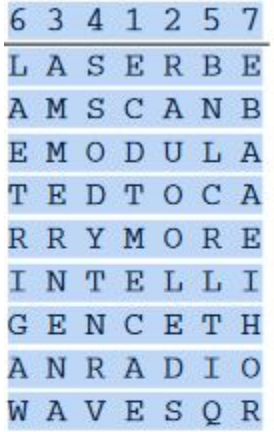
We wish to encipher the message LASER BEAMS CAN BE MODULATED TO CARRY MORE INTELLIGENCE THAN RADIO WAVES

The message is written out on a width of 7, under the numerical sequence.

Adding two dummy letters, say Q and R………….



6	3	4	1	2	5	7
L	A	S	E	R	B	E
A	M	S	C	A	N	B
E	M	O	D	U	L	A
T	E	D	T	O	C	A
R	R	Y	M	O	R	E
I	N	T	E	L	L	I
G	E	N	C	E	T	H
A	N	R	A	D	I	O
W	A	V	E	S		



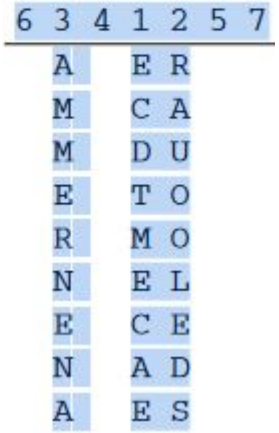
6	3	4	1	2	5	7
L	A	S	E	R	B	E
A	M	S	C	A	N	B
E	M	O	D	U	L	A
T	E	D	T	O	C	A
R	R	Y	M	O	R	E
I	N	T	E	L	L	I
G	E	N	C	E	T	H
A	N	R	A	D	I	O
W	A	V	E	S	Q	R

Transposition Ciphers

Now the enciphering process consists of reading out the cipher text vertically in the order of the numbered columns. At the same time it can be written in groups of five letters.

ECDTM ECAER AUOOL EDSAM MERNE NASSO DYTNR VBNLC RLTIQ
LAETR IGAWE BAAEI HOR

The decipherer Process: Count the number of letters in the message (63).
Since the length of the key is 7, the dimensions of the inscription rectangle are 7 × 9.
When the complete message has been entered, the plain text appears in normal order.



6	3	4	1	2	5	7
	A		E	R		
	M		C	A		
	M		D	U		
	E		T	O		
	R		M	O		
	N		E	L		
	E		C	E		
	N		A	D		
	A		E	S		

Product Ciphers

- Two substitutions make a more complex substitution
- Two transpositions make more complex transposition
- But a substitution followed by a transposition makes a new much harder cipher

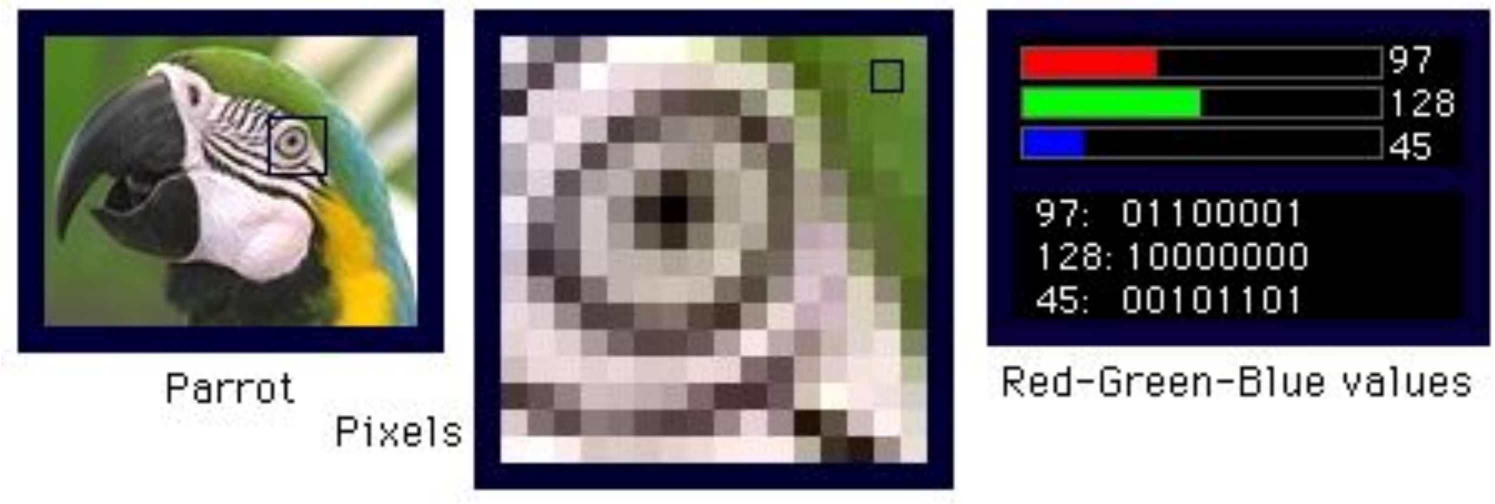
- Uses a sequence of substitutions and transpositions
  - Harder to break than just substitutions or transpositions
- This is a bridge from classical to modern ciphers.

One Time Pad

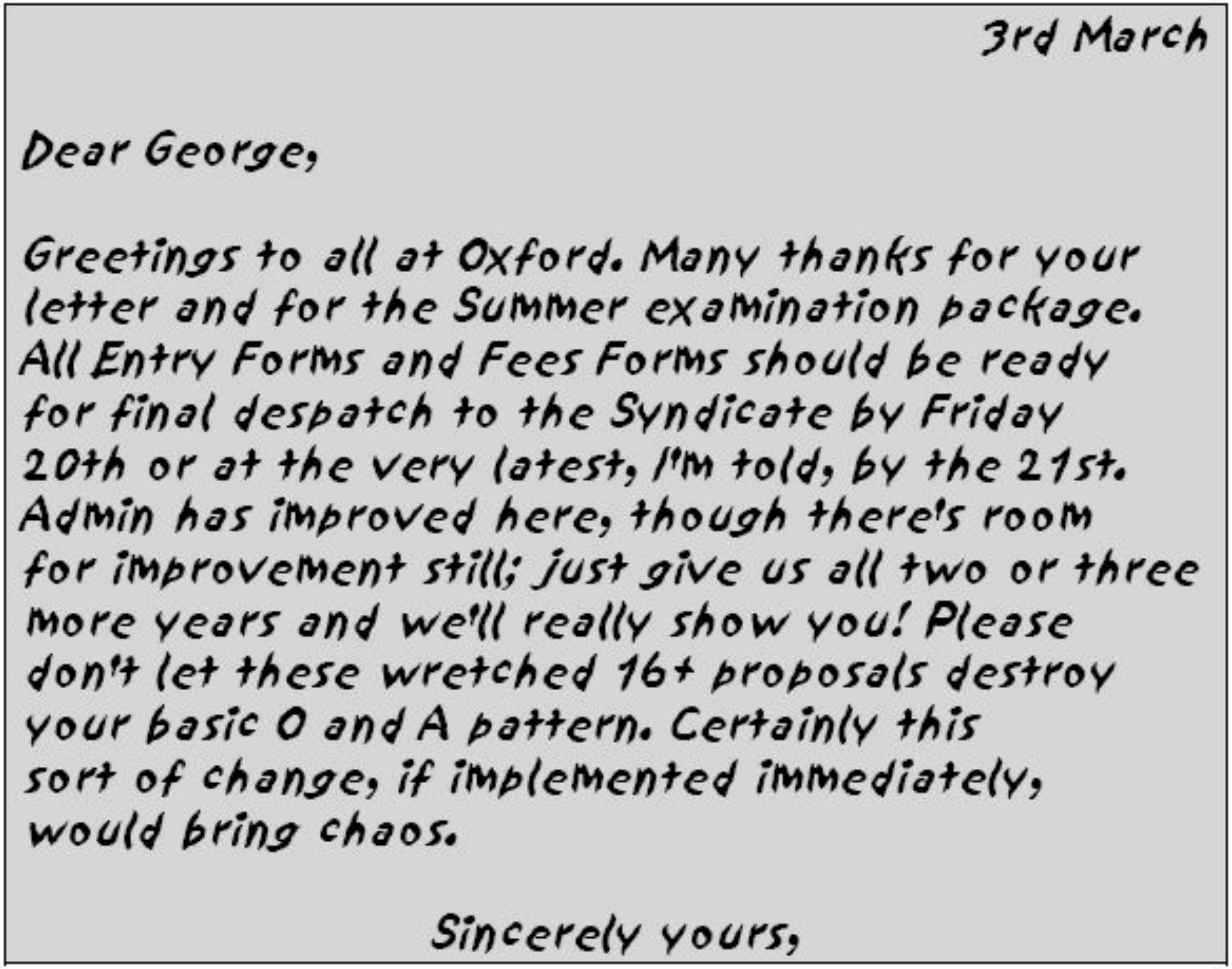
- Each plain text symbol is encrypted with a key randomly chosen from a key domain.
- The key has the same length as the plaintext and is chosen completely in random.
- There is the practical problem of making large quantities of random keys
- Another problem is key distribution and protection
- Key can be used once

Steganography

- Hide a message in another message.
- E.g., hide your plaintext in a graphic image
  - Each pixel has 3 bytes specifying the RGB color
  - The least significant bits of pixels can be changed w/o greatly affecting the image quality
  - So can hide messages in these LSBs
- Advantage: hiding existence of messages



- Take a 640x480 (=30,7200) pixel image.
- Using only 1 LSB, can hide 115,200 characters
- Using 4 LSBs, can hide 460,800 characters.



3rd March

Dear George,

Greetings to all at Oxford. Many thanks for your
letter and for the Summer examination package.
All Entry Forms and Fees Forms should be ready
for final despatch to the Syndicate by Friday
20th or at the very latest, I'm told, by the 21st.
Admin has improved here, though there's room
for improvement still; just give us all two or three
more years and we'll really show you! Please
don't let these wretched 16+ proposals destroy
your basic O and A pattern. Certainly this
sort of change, if implemented immediately,
would bring chaos.

Sincerely yours,

Figure 2.8 A Puzzle for Inspector Morse
(from *The Silent World of Nicholas Quinn*, by Colin Dexter)

Hides existence of message

- Using only a subset of letters/words in a longer message marked in some way
- Using invisible ink

Summary

- Have considered:
  - classical cipher techniques and terminology
  - monoalphabetic substitution ciphers
  - cryptanalysis using letter frequencies
  - Playfair cipher
  - polyalphabetic ciphers
  - transposition ciphers
  - product ciphers
  - stenography