# Cryptography

Women in Science yr 12/13

Oxford

April 2009

Dr Audrey Curnock

# Cryptography in everyday life

- Internet banking
- On-line/phone credit/debit card purchases
- Cashpoints/ATMs
- Shopping using pin numbers on credit/debit cards
- Remote log-ons ….companies, universities…

# Why do we need cryptography?

- Alice

Bob

Alice has a message m (plaintext) that she wants to send to Bob.

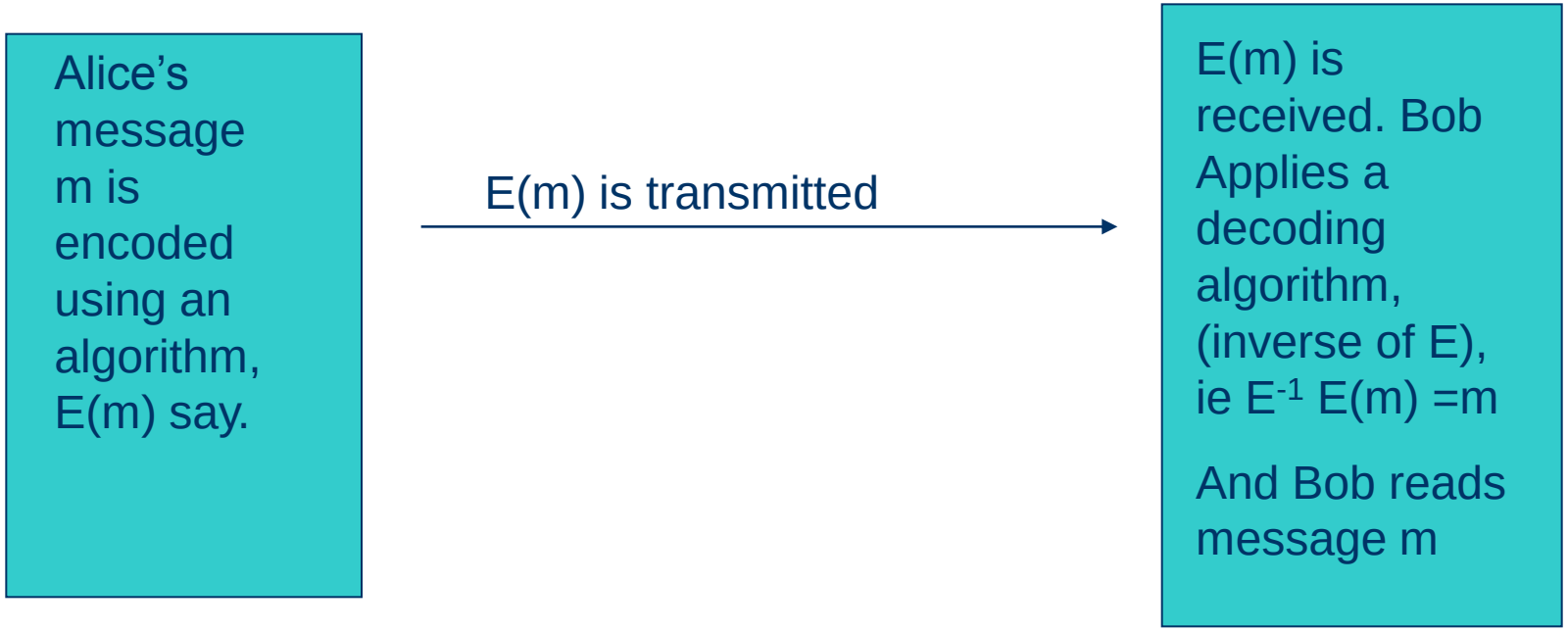
Alice's priorities are
1) Privacy (no-one reads/intercepts her message)
2) Data is received by Bob, it's definitely from Alice (authenticated) and is correct (hasn't been altered in transit).

# In *Ideal World…*

- Message m is transmitted.
- No-one can see it, no-one can alter it.
- User's (Alice's) transmission is successfully received and can be read (by Bob).

# How is cryptography used?

- Alice and Bob both have a KEY (secret)



# Earliest Ciphers – Substitution Cipher

- Each letter is substituted for another. In effect a *bijection* assigns a new letter for each letter of alphabet.
- Call this bijection π – it's a permutation

It's helpful to use a grid as in appendix 1.

**<u>Example 1</u> : Caesar Cipher.**

Each letter of alphabet is shifted along by 3

# Plaintext and Ciphertext Using a Caesar Cipher (K=3)

- CAT =
- I HAVE A CAT =
- I CAME I SAW I CONQUERED=

- KHOOR =
- WHEDUHDN=

**Example 2**: Jane Austen - See the grid in Appendix 2

# Modular Arithmetic

- Gauss introduced this “clock arithmetic" in about 1801.
- Example : in modular 5 we use digits 0,1,2,3,4 and all integers are written as one of the values, “mod”5.
- 7 is 2 mod 5, 20 is 0 mod 5
- $3^2 = 4 \bmod 5$ and so 136 = 1 mod5.
- Caesar Code : $\pi(x) = (x+3) \bmod 26$.

- See the appendix 3 for examples and proofs

# How safe is this?

- In English “E” is a very frequently occurring letter…so given a longish string we can guess what “E” maps to. Then letters T, A, etc Frequency of a letter is preserved under this cipher.
- In the Caesar cipher both parties need to know the key “k=3” is usual shift. Could be any key (possible 26 choices).
- How many distinct substitution ciphers would there be? (usual roman alphabet). Approx $4 \times 10^{26}$

# Frequency Analysis

- There are published tables giving the expected frequency (%) of singles, doubles and triple letter combinations
- Using these we can “break” a substitution cipher – more words, the easier
- Note : it’s usual to send/write cipher text in blocks of a certain size “n-tuples” = words of length n.

# Letter frequency tables – in descending order

| Letter | % frequency | Doubles | Triples |
|---|---|---|---|
| E | 12.7% | TH | THE |
| T | 9% | HE | ING |
| A | 8.2% | IN | AND |
| O | 7.5% | ER | HER |
| I | 7% | AN | ERE |
| N | 6.7% | RE | ENT |

# Enigma Machine- Rotor Cipher machines

- After WWI mechanical substitution ciphers were patented
- Most famous was Enigma machine used by the Germans
- At Bletchley Park Alan Turing and his colleagues developed systems to break these codes, and “Colossus” the first mechanical computer was built.

# Better Ciphers using Modular Arithmetic

- We use an integer for each letter of the alphabet, so for A,B,C…Z we need integers 0,1,2,…25 say.

**Example 3 : Polyalphabetic cipher**

Using blocks of n=3

Let K = $\{\pi_1, \pi_2, \pi_3, \}$ where $\pi_1(x) = x + 3$,

$\pi_2(x) = x + 5$ and $\pi_1(x) = x + 8$ .

Plaintext = I HAVE A CAT. Find the ciphertext

IHA VEA CAT = 8 7 0 21 4 0 2 0 9

# Polyalphabetic Ciphers: Vignère Cipher

- Choose a secret key word - short string of letters. Eg HERRING
- A  Vignère cipher is found by adding the secret code one letter at a time to the plaintext. Here letter frequency will not be preserved

**Example 4** : Using the Key HERRING translate

Plaintext = MEET ME AT THE BAR (use blocks of 3).

# RSA : Public-Key Encryption

- So far we've looked at symmetric encryption – both sender and receiver have same key.
- public key is asymmetric encryption
- There are two keys – public and private
- Uses large primes – given the product of two large primes N it is thought to be infeasible to be able to factorise N into primes p,q and so computational unbreakable

# Steps to using RSA

- Compute N = pq
- Compute (p-1)(q-1)
- Find integer e which is co-prime to (p-1)(q-1)

- (N,e) = Public key
- Find the integer d, multiplicative inverse to e modulo (p-1)(q-1)

# Steps to using RSA

- Suppose message to be sent is m (plaintext)
- $C = m^e \pmod{N}$ for encrypting
- $m = c^d \pmod{N}$ for decrypting
- (d, p, q) = Private Key
- (use digits A=01, B=02,….Z =26)

# Appendix :
# Brief foray into modular arithmetic

We need three main mathematical tools :

- Simple exercises on Modular arithmetic,
- finding multiplicative inverses,
- modular exponentiation.

Notes are appended.

# Further Reading


1. M. Bellar, *Modern Cryptography*

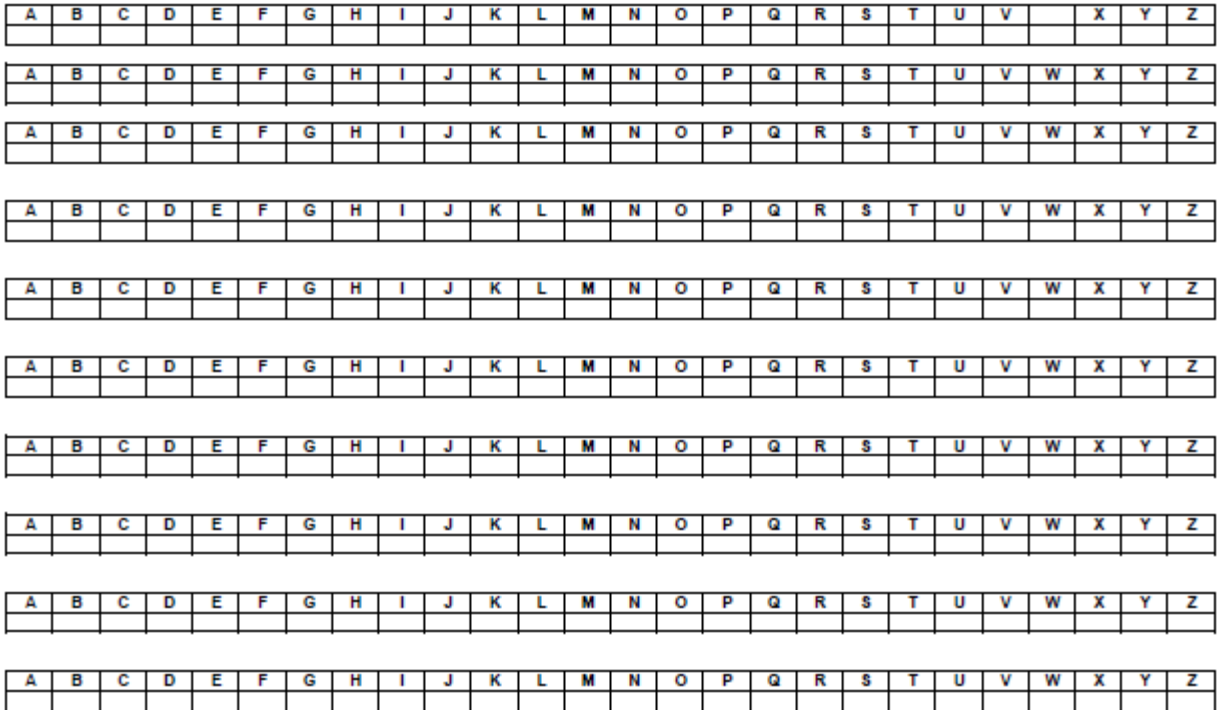
See www-cse.ucsd.edu/users/mihir/cse2007

2. P.J. Cameron, Introduction to Algebra, OUP, 1998
3. T. Körner, *Coding and Cryptography Notes*

   See www.dpmms.cam.ac.uk/~twk
4. Y. Lindell, *Introduction to Cryptography,* Bar-Ilan University,Israel,2006
5. A. Menezes, P. Van Oorschot and S. Vanstone, *Handbook of Applied Cryptography*, 1996
6. E. Oswald and N. Smart, *Historical Ciphers,* Lecture Course COMS30124 Notes, University of Bristol 2006
7. Sarah Flannery, *In Code, a mathematical journey*, Profile Books LTD, 2000.

# Appendix 1

**USEFUL LETTER GRID**



# Appendix 2

**Ciphertext: translated piece from a Jane Austen novel using a Substitution Cipher**
**For ease of deciphering I have left natural word spacings**

**Exercise : Try to break this piece of secret code**

| | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| L | S | P | G | H | I | L | A | O | | D | H | Z | | A | V | V | | T | B | J | O | | | |
| E | | | | A | | E | T | | | | A | | | T | O | O | | | | | | | | |
| L | T | I | H | Y | Y | H | Z | Z | L | K | | A | V | | Z | H | F | | H | | D | V | Y | K |
| E | | | A | | | A | | | E | | | T | O | | | | | | A | | | | | |
| H | M | A | L | Y | | H | | Z | O | V | Y | A | | W | H | B | Z | L | | | | | | |
| A | | T | E | | | A | | | | | | T | | | A | | | E | | | | | | |
| O | L | Y | | J | V | T | W | H | U | P | V | U | | H | K | K | L | K | | | | | | |
| | E | | | | | | | | | | | | | A | | | E | | | | | | | |
| F | V | B | | H | Y | L | | A | V | V | | N | L | U | L | Y | V | B | Z | | A | V | | |
| | | | | A | | | | T | O | O | | | E | | E | | | | | | T | O | | |
| A | Y | P | M | S | L | | D | P | A | O | | T | L | | P | M | | F | V | B | Y | | | |
| T | | | | | E | | | | T | | | | E | | | | | | | | | | | |
| M | L | L | S | P | U | N | Z | | H | Y | L | | Z | A | P | S | S | | D | O | H | A | | |
| | E | E | | | | | | | A | | E | | | T | | | | | | | A | T | | |
| A | O | L | F | | D | L | Y | L | | S | H | Z | A | | H | W | Y | P | S | | | | | |
| T | | E | | | | E | | | | | A | | T | | A | | | | | | | | | |
| A | L | S | S | | T | L | | Z | V | | H | A | | V | U | J | L | | | | | | | |
| T | E | | | | | E | | | | | A | T | | | | | E | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | | | |

Hints ; guess letters in the following order
S –
Y –
P–
now look for whole words

# Appendix 2 ctd

Letter Frequency Analysis for ciphertext from Jane Austen novel

| | |
|---|---|
| A | 15 |
| B | 5 |
| D | 5 |
| F | 4 |
| G | 1 |
| H | 17 |
| I | 2 |
| J | 3 |
| K | 5 |
| L | 22 |
| M | 4 |
| N | 2 |
| O | 7 |
| P | 6 |
| S | 9 |
| T | 5 |
| U | 5 |
| V | 15 |
| W | 3 |
| Y | 13 |
| Z | 11 |
| total | 161 |

Sorted data

| | |
|---|---|
| L | 22 |
| H | 17 |
| A | 15 |
| V | 15 |
| Y | 13 |
| Z | 11 |
| S | 9 |
| P | 6 |
| O | 7 |
| B | 5 |
| D | 5 |
| K | 5 |
| T | 5 |
| U | 5 |
| F | 4 |
| M | 4 |
| J | 3 |
| W | 3 |
| I | 2 |
| N | 2 |
| G | 1 |