Cryptography – better don’t get confused!

1. Short introduction

Namely, why has concealing messages been so important?
Not only recently, but over the centuries.
There are numerous applications:

- military purposes (e.g. spies)
- credit cards, bank accounts
- computer passwords
- diplomacy
- leisure: cryptograms – quizzes/puzzles with encrypted text

2. Meaning

We will talk about two different things (the former one in detail, the latter one rather shortly).
‘cryptography’ comes from Greek:
κρυπτός, *kryptos*, “hidden, secret”
γράφω, *gráphō*, “I write”
Hence, cryptography enables us to send an encoded (encrypted) message in such a way, that no one can decipher it without a code – which is usually really hard to crack. In other words, it obscures the meaning of the message, but it does not conceal the fact that there is a message – in contrary to ‘steganography’.
‘Steganography’ also comes from Greek and means “covered, or hidden writing”. This is even more interesting, as it enables us to write the message in such a way that no one apart from a few informed people even realizes there is a hidden message. In general, steganographic message will seem to be something else: a picture, an article, a shopping list, etc.

Examples of steganography (only two in the presentation):

- first documented applications as long ago as 440 BC reported by Herodotus:
  - wooden panels with information covered in wax (the recipient must scratch the wax first in order to read the message).
  - message tattooed on the head; obviously the messenger must wait until the hair grows again to conceal the message.
- invisible ink that can be made visible by means of UV light or some acidic solutions or vapours.
- pictures: small changes on the pixel level (e.g. colour of every 10th pixel is changed, each colour corresponds to a different letter). It is impossible to notice for an unaware observer.
- Bacon’s cipher: every letter of the alphabet is expressed as a 5-digit configuration of As and Bs. The fake message is then written using two different typefaces (or fonts), each corresponding to A or B. The pattern of the two typefaces corresponds to the order of As

and Bs which in turn corresponds to the letters of the alphabet. (Some people claim it was Bacon who wrote Shakespeare’s plays. They also say he encrypted this information using his own cipher and the encrypted text is included within the plays. [See http://en.wikipedia.org/wiki/Bacon%27s_cipher.])

3. More about cryptography

In the next part of this presentation we will focus on the cryptography only.
We can distinguish few basic methods of cryptography:

- code words

  Different expressions have got different meanings, e.g.:
  - *apple pie* means *prepare the attack* (in military environment)
  - *mum’s favourite broom* means *enemies*

- transposition cipher

▪ need a break	->	ende a rbaek	or	edne a rabek
▪ have a sandwich?	->	ahev a asndiwhc?	or	aehv a adihsnwc?

  The above examples are fairly simple as both rules are rather straightforward – in the first example divide each word into letter pairs and swap letters in each pair. In the latter, proceed as in the first method, then repeat it, but excluding the outermost letter on either side, then proceed again, this time excluding two outermost letters on either side, etc. Either way, this cipher does not change the letters in the message, only their position within a word. Hence, it is not really a safe method of encoding.

- substitution cipher

  Replaces each letter with the one *n* places to the right or left in the alphabet:
  - *fly* becomes *gmz* (1 place to the right)
  - *banana* becomes *xvjvjv* (4 places to the left)

  Caesar cipher (a particular type of the substitution cipher): the shift is 3 places to the right, e.g.:

  Every rainbow has got two ends becomes *Hzhub udlqery kdw jrv vyr hqgw.*

  This particular example of the substitution cipher is named after Julius Caesar, who happened to use it to communicate with his generals. Was rather successful, since most of the people were illiterate at the time!

- symbolic cipher

  Every letter is assigned to a symbol, e.g.:

  I am making a snowman tomorrow

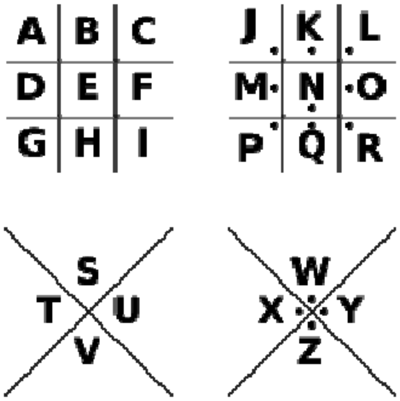
  becomes

I am making a Snowman tomorrow

(The following two ciphers were not used in the presentation.)

- pigpen cipher

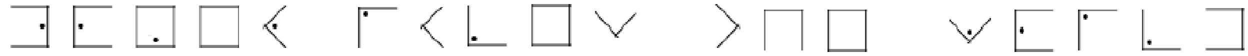
  Every letter is assigned to a symbol (see the grid).



  Hence,

  Money rules the world

  becomes

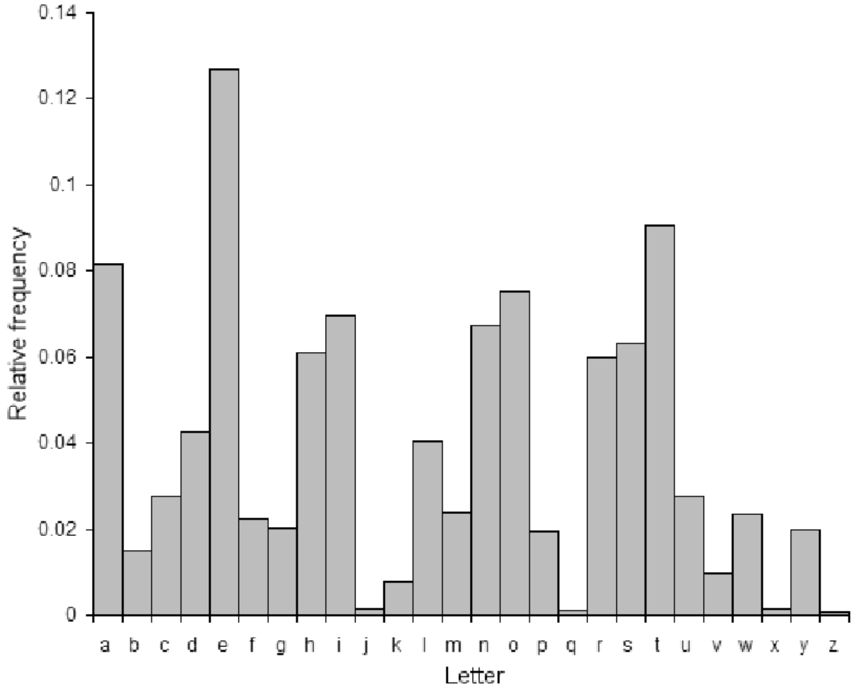


  (See http://en.wikipedia.org/wiki/Pigpen_cipher.)

- polyalphabetic ciphers

  First described in 1467; best example: Vigenere's cipher. In general, it uses the substitution cipher, but with changing shifts (which change according to some rule).

Nonetheless, all of these are fairly easy to break – frequency analysis:



(See http://en.wikipedia.org/wiki/Frequency_analysis.)

Simplifying the theorem, since *e* and *t* occur in English most often, in the encrypted text the letters corresponding to *e* and *t* should occur most often as well. Similarly, the letters corresponding to the rarest letters in the alphabet (namely, *z* and *q*) are not supposed to occur in the encrypted message with high frequencies.
Usually text of 50 characters should be enough to decrypt the message. That is less than in the previous sentence! This is why people introduced far more complicated ways of encrypting messages. This is where Mathematics comes into light. There are quite a few methods of encrypting messages mathematically. We will focus on one of them, called RSA, and to be more precise, we will consider its simplified version, called Kid-RSA.

4. Kid-RSA

RSA stands for the names of its creators: Ron Rivest, Adi Shamir and Leonard Adleman, all of whom were professors at the Massachusetts Institute of Technology (MIT) in USA. The method was first described in 1977 and is considered to be one of the two most popular algorithms.
Kid-RSA, however, is the simplified version of the above proposed by Neal Koblitz.
Before we start, we have to explain some terms that will be used here:

- integer
- modulo of a number
- public key/private key: public key is widely known, private key is kept confidentially (just as their names suggest). Public key is for encrypting, whereas private key is for decrypting messages; this means that anyone can encrypt the message, but only a few people can actually decrypt it. Important: the two keys are different! There is a mathematical relationship between them, but it is extremely hard to find. Hence, no one knowing the public key can really tell what the private one is.
- plaintext and ciphertext: the former is the original, unchanged message whereas the latter is the encrypted message
- cipher: a procedure you have to follow step by step in order to conceal your text
- encryption (plaintext -> ciphertext)
- decryption (ciphertext ->plaintext)

And now comes the most important part, namely how the Kid-RSA works…
(See http://www.cs.uri.edu/cryptography/publickeykidkrypto.htm.)

A person (Alice) chooses four numbers *a*, *b*, *A*, and *B*. Then Alice calculates the following:
(*e* stands for 'encryption', whereas *d* stands for 'decryption')
$M = a * b - 1$
$e = A * M + a$
$d = B * M + b$

$n = (e * d - 1) / M = A * B * M + a * B + A * b + 1$

Now Alice's public key is (n, e) and her private key is d.
To send a plaintext P to Alice, one uses function $C = e * P *$ (mod n).
Alice can then decipher the ciphertext by using function $P = C * d *$ (mod n).
Note: The plaintext has to be a number in the range of 0 to n-1. So for this system to work the plaintext or blocks of plaintext have to be converted into numbers in the range of 0 to n-1. Since Alice publishes e and n, anyone who wants to send encrypted messages to Alice can do so, but these messages cannot be decrypted without knowledge of d. d is kept secret and only Alice knows it, so only she can decrypt messages.

(Some links where everything is explained in more detail:
http://www.scribd.com/doc/2345053/Modular-Arithmetic-RSA-Encryption
http://www.math.washington.edu/~koblitz/crlogia.html
http://www.cs.uri.edu/cryptography/publickeykidkrypto.htm
http://www.mathaware.org/mam/06/Sauerberg_PKC-essay.html)