Linnaeus universitet
Department of Computer Science
OF

2016-01-21

Encryption

Practical work #1, 1DV700, VT16

In this practical work you are to investigate how to implement different encryption algorithms and test how resilient they are to crypto analysis.

You may do this practical work individually or in a group of two students. Read the information "Instructions for practical assignments" in MyMoodle before you start the work.

1. The first task is to investigate different terms within cryptography and related areas.

a) What are the differences between the following pairs of methods;

Symmetric encryption – Asymmetric encryption
Encryption algorithms – Hash algorithms
Compression - Hashing

b) What are the differences between Steganography (read document about steganography in MyMoodle), Encryption and Digital Watermarking? What is the purpose of each method and when are they used?

2. What is the message hidden in the text below (using Steganography)?

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 dispatch 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,

("The Silent World of Nicholas Quinn", by Colin Dexter)

3

a) Decrypt the message HKPUFCMHY BHDDXZH with the help of this simple substitution key (cipher line).

plain	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
cipher	X	G	P	Y	H	Q	Z	I	R	A	J	S	B	K	T	C	L	U	D	M	V	E	N	W	F	O

b) Can this message be decrypted by someone not having the key? Motivate!

4. Write a Java program, implementing encryption/decryption without using the java.security package. The program should ask the user for encryption method, if you want to perform encryption or decryption, secret key and a text file to process. The output should be a processed file. You should implement at least two simple encryption methods, one substitution and one transposition method. For the substitution method, keep key sizes at maximum equivalent to eight bits, i.e. 2^8=256 different possible keys. Make sure that you can both encrypt and decrypt files with your program.

5. Download the file "plaintext.txt" found on the course home page. Add a secret message at the end of the file, at least one page long, and the names of the students that created the file. Encrypt the updated file using your program (you may select any method you have implemented). Post the encrypted file in the folder "Cipher texts". The name of the file should be the name of the student uploading the file.

6. In the folder mentioned above you will find cipher texts from the other groups. Download some of these and try to perform crypto analysis on them. You may use any tool or method to perform this task. When you have successfully analysed at least one of the files, include a description of how you did it in the report.

7. Below you find the pseudo code for a hash function.

```
unsigned int hash(bytearray[] msg)
{
   unsigned int hash = 0xDECAFBAD;
   for(i = 0; i < msg.length(); i++)
   {
      hash = ((hash << 5) XOR (hash >> 27)) XOR msg[i];
   }
   return (hash BITWISE-AND 0x7FFFFFFF);
}

(x << 5 means 5 bits shift to the left, shifting in zeros,
>> is shift right)
```

a) Explain in words and/or with a figure how the function works.

b) Is this a good cryptographic hash function? Motivate your answer!

The report you write for this practical work should include your results on all the tasks. Format the report with a title page, table of content etc. Your answers to the questions should elaborate on the answers. For instance when you write about your program you should describe the algorithms you have implemented and how the program works. For task 6 you should explain the tools or methods used and what worked as well as what didn't work during the crypto analysis.
Make a zip archive with report and source code for the program.
Post the report and source code in the upload folder assigned for it at latest February 7.