Linnaeus universitet 2013-01-28
DV
OF

Laboration #1 Kryptering
1DV425, VT13

I denna laboration arbete ska ni undersöka hur man kan använda och implementera olika krypteringsalgoritmer samt testa hur motståndskraftiga de är att kryptoanalys.

Du kan göra detta arbete enskilt eller i grupp om två studenter.

1. Den första uppgiften är att undersöka olika termer inom och närliggande till kryptering.
a) Vad är det för skillnader mellan följande par av metoder:
symmetrisk kryptering – asymmetrisk kryptering
krypteringsalgoritmer – hashfunktioner
komprimering – hashning
b) Vad är skillnaderna mellan kryptering, steganografi och digital vattenmärkning? Vad är syftet med de olika metoderna och när används de?

2. Vad är för budskap som är gömt i texten nedan (med hjälp av steganografi)?

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) Dekryptera meddelandet HKPUFCMHY BHDDXZH med hjälp av följande enkla substitutionsnyckel:

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) Kan detta meddelande knäckas av någon som inte har nyckeln? Motivera!

4. Skriv ett program i valfritt programmeringsspråk som implementerar kryptering/de-kryptering. Du får inte använda några inbyggda krypteringsalgoritmer utan du måste implementera dem helt själv. Du ska skapa minst två enkla krypteringsmetoder, en med substitution och en med transposition. Nyckelstorleken ska vara väldigt liten och maximal motsvara åtta bitar, dvs $2^8 = 256$ olika möjliga nycklar (Det motsvarar t.ex. ett tecken som nyckel). Programmet ska fråga användaren om önskad krypteringsmetod, om du vill utföra kryptering eller dekryptering, den hemliga nyckeln samt namnet på en textfil som programmet sedan läser in. Utdata ska vara den bearbetade filen. Se till att du både kan kryptera och dekryptera filer.

5. Ladda ner filen "plaintext.txt" från kursens hemsida. Lägg till ett hemligt meddelande, minst en sida långt, i slutet av filen och namnen på den eller de elever som skapade filen. Kryptera den uppdaterade filen med ditt program (du kan välja valfri metod som du har implementerat). Zippa och skicka den krypterade filen till Ola.Flygt@lnu.se med namnet "Cipher_xxxxxxxx.txt" där xxxxxxx är ditt användarnamn på Lnu.

6. Efterhand som det kommer in krypterade filer så lägger jag upp dem på kursens hemsida. Ladda ner dessa och försöka utföra kryptoanalys på dem. Du kan använda valfritt verktyg och metod för att utföra denna uppgift. Det räcker att du knäcker krypteringen på en av filerna. Förklara hur du knäckte den och vilken form av krypteringsmetod det är som du knäckt.

7. Nedan pseudokod är en implementering av en hashfunktion:

```
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 innebär 5 bits shift till vänster där man skiftar
in nollor, >> är shift åt höger)
```

a) Förklara i ord eller med en figur hur funktionen fungerar.

b) Är det här en bra kryptografisk hashfunktion? Motivera ditt svar.

Rapporten du skriver för den här laborationen ska inkludera dina resultat på alla uppgifter. Formatera rapporten med en titelsida, innehållsförteckning mm. Det räcker inte med korta svar utan du ska utveckla svaren mer. Gör ett zip-arkiv med rapport och källkoden för programmet och skicka till Niclas Håkansson <nh222aq@student.lnu.se>. Sista datum för inlämning är tisdagen den 12 februari.