| UNIVERSITY OF Southampton<br>Electronics and Computer Science | | ***Coursework Instructions 2012/13*** |
|---|---|---|
| **Module: ELEC6032** | **Cryptography** | **Dr D A Nicole<br>Dr Basel Halak** |
| **Assignment: 1 of 1** | **Contribution to Module: 50%** | **Due Date: 07/05/13** |

## Instructions

This coursework is in four parts. You should complete each part, working independently of other individuals.

**1.** Decrypt the hidden message contained in this image:

```
D1 C1 8D 43 E3 C6 C3 58 F7 C0 95 4A F2 DD 9A 5C A4 DC 91 43 F2 C1 8A 48 A4 D4 96 48
E8 93 96 54 ED C1 C3 5D F1 C1 C3 5C E3 D6 81 5B F0 C1 85 5D A4 C1 8A 4C F5 C1 82 4A
F6 93 8F 48 E3 93 84 4F EA D4 C3 54 A4 D2 91 50 A4 D6 91 5C E7 C5 86 54 E3 D1 86 56
A4 C5 9A 43 E5 C1 85 5C A4 C3 8D 5B A4 D5 80 5F F6 DD 92 1A F7 D6 81 40 A4 D0 91 5F
E2 D1 82 1A E3 D1 C3 59 F6 D6 85 58 E5 93 B3 54 E2 C1 85 1A E6 C0 C3 5D F1 C1 C3 4C
E5 C0 91 4A E3 C5 81 5B A4 C9 8D 56 A4 C3 81 40 F6 93 90 5F E6 C9 C3 4A E6 D2 84 54
F4 D4 C3 50 F2 D4 96 1A EA D2 95 40 EA CA 85 1A EA D2 92 1A EB C5 86 4B E2 9D C3 6F
E6 D9 91 53 F6 D6 CF 1A F2 C0 C3 5D F1 C1 C3 53 F2 D6 8B 5C A4 C3 8D 5B A4 D5 80 5F
F6 DD 92 1A EB C1 84 50 F6 C1 82 1A E7 C1 81 59 FD C1 C3 4C E3 93 80 58 E2 C1 85 1A
EA 93 99 52 F4 C6 C3 40 E6 D6 91 1A E2 C1 86 4C E6 DB 85 1A E3 C6 86 48 EA D4 CD 1A
C6 D2 91 1A E7 C1 86 5C E6 D2 C3 4C E5 93 84 4F F6 93 AB 62 A4 C5 85 1A E3 C6 81 52
F0 C6 84 1A E3 D1 C3 4F EA DA 91 1A F4 DD 8B 4E F1 D4 C3 5D F1 C1 C3 4C E5 C0 91 4A
E3 C5 81 5B A4 C0 86 58 FE 93 8D 1A E1 C1 9A 54 E3 C5 8A 48 AA 93 B6 58 EE C1 8A 48
E1 9F C3 58 F7 C0 95 4A F2 DD 9A 5C A4 D5 8D 56 A4 D4 96 48 A4 D4 96 5F F6 DD 84 1A
E3 D1 C3 5D F1 C1 C3 50 F1 D1 9A 48 A4 D0 81 59 EC CA 8D 5D F2 D1 82 1A E1 C1 99 54
F2 D2 85 1A ED C1 86 56 A4 CA 81 50 AA 93 A4 4F F6 D6 91 1A F1 DD 8A 48 A4 DC 91 48
E5 93 82 4C E5 C1 C3 4A E6 D2 90 4C E1 C9 91 4B A4 C3 8D 5C F6 D5 C3 58 F7 93 84 4F
F6 93 95 5B F7 C1 93 5D F2 D1 82 1A EA D6 81 52 E5 C2 C3 5D F1 C1 C3 50 E6 D6 9A 4B
AA 93 AF 58 EC 93 96 54 ED C1 C3 5B E6 D9 C3 5C EC C3 93 48 E2 D5 90 52 FD CA 8F 1A
F5 C1 93 4C E7 C6 91 5F F6 C2 C3 5D F1 C5 85 1A FE C1 85 5C EA C7 91 14
```

**Hint**: the above message is encrypted using two stage encryption system, the first stage is unknown, but the second stage is an LFSR cipher with a degree 5). You are given the first two characters of the output of the first encryption stage: Ur

**2.** a. At least one of the following polynomial is a generator polynomial for a Hamming code, which are they? Justify your answer

$$f1(x) = X^6 + X^3 + X^2 + X + 1$$

$$f2(x) = X^6 + X^5 + X^4 + X^3 + 1$$

$$f3(x) = X^6 + X^5 + X$$

$$f4(x) = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$$

$$f5(x) = X^6 + X + 1$$

b. Construct the H and G matrix of a Hamming code (63, 57) based on your answer of 2-a

c. Based on your answers of 2-a and 2-b, are any of the following messages a valid code word?

m1 = 101001111000000000000000000000000000000000000000000000000000000

m2 = 100001100000000000000000000000000000000000000000000000000001000011

m3 = 100001100000000000000000000010000000000000000000000000000001000011

**3.** Decrypt the following message:

Wvzi Hzizs R zn dirgrmt gl zkkob uli gsv kiltiznnvi klhrgrlm zwevigrhvw rm gsv Grnvh Fmrlm. Zh ivjfvhgvw R zn vmxolhrmt z xlnkovgvw qly zkkorxzgrlm, nb xvigrurxzgrlm nb ivhfnv zmw gsivv ivuvivmxvh Gsv lkkligfmrgb kivhvmgvw rm gsrh orhgrmt rh evib rmgvivhgrmt zmw R yvorvev gszg nb hgilmt gvxsmrxzo vckvirvmxv zmw vwfxzgrlm droo nzpv nv z evib xlnkvgrgrev xzmwrwzgv uli gsrh klhrgrlm Gsv pvb hgivmtgsh gszg R klhhvhh uli hfxxvhh rm gsrh klhrgrlm rmxofwv R szev hfxxvhhufoob wvhrtmvw, wvevolkvw, zmw hfkkligvw orev fhv zkkorxzgrlmh R hgirev uli xlmgrmfvw vcxvoovmxv R kilerwv vcxvkgrlmzo xlmgiryfgrlmh gl xfhglnvi hvierxv uli zoo xfhglnvih Drgs z YH wvtivv rm Xlnkfgvi Kiltiznnrmt, R szev z ufoo fmwvihgzmwrmt lu gsv ufoo oruv xbxov lu z hlugdziv wvevolknvmg kilqvxg R zohl szev vckvirvmxv rm ovzimrmt zmw vcxvoormt zg mvd gvxsmloltrvh zh mvvwvw Kovzhv hvv nb ivhfnv uli zwwrgrlmzo rmulinzgrlm lm nb vckvirvmxv Gszmp blf uli blfi grnv zmw xlmhrwvizgrlm R ollp ulidziw gl hkvzprmt drgs blf zylfg gsrh vnkolbnvmg lkkligfmrgb Blf szev mld ivzxsvw gsv vmw lu gsrh nvhhztv

**4.** Select a recent serious incident of failure of a cryptographic system or a new type of attack on such a system. You may choose from incidents associated with AES, 3-DES , *Mifare*, *DESfire* or *WEP*. For your chosen incident or attack:

   a. Carefully describe the nature of the incident, with special reference to the cryptographic techniques used, both in attempting to secure the system and in penetrating it.

   b. Can you identify any current deployments which still have this vulnerability?

## Submission

Please submit a `.zip` file containing your report in PDF format using the ECS electronic hand-in system, C-Bass, by 11pm on the due date. The `.zip` file should also contain any additional software or electronic material you have created. Your report should amount to about 2000 words excluding references and should clearly describe your approach to each task. You may make free, acknowledged, use of information and code from the WWW or other publications. You should work alone for the exercises and writeup.

## Module Learning Outcomes (MLOs)

Having successfully completed the module, you will be able to:

1. Provide an overview of cryptographic techniques
2. Explain the constraints and limitations of secure systems.
3. Describe the trade-off between usability and security of a system.

## Marking Scheme

| Criterion | Description | Outcomes | Marks |
|---|---|---|---|
| Challenge 1 | The thoroughness of deciphering methodology and the accuracy of the solution | 1,2 | 25 |
| Challenge 2 | The thoroughness of methodology and the accuracy of the solution | 1,2 | 25 |
| Challenge 3 | The thoroughness of methodology and the accuracy of the solution | 1,2 | 25 |
| Challenge 4 | Thoroughness of Research and accuracy of description | 1,2,3 | 25 |

*You should expect to spend up to 100 hours (fifteen working days) each on this assignment.*

*Your attention is drawn to the University regulations concerning academic integrity, late penalties, and extensions.*

.