PMAT 329 Introduction to Cryptography ASSIGNMENT 2

Set: Wednesday , Nov 3, 2004

Due: Wednesday , Nov. 17, 2004
Total: 60 points

1. [12 points] Cryptanalyze the following polyalphabetic ciphertext. Show your work. Note that this ciphertext is the example used in the handout given out in class to illustrate the factoring method for resolving the number of alphabets.

```
SIJYU MNVCA ISPJL RBZEY QWYEU LWMGW ICJCI MTZEI MIBKN
QWBRI VWYIG BWNBQ QCGQH IWJKA GEGXN IDMRU VEZYG QIGVN
CTGYO BPDBL VCGXG BKZZG IVXCU NTZAO BWFEQ QLFCO MTYZT
CCBYQ OPDKA GDGIG VPWMR QIIEW ICGXG BLGQQ VBGRS MYJJY
QVFWY RWNFL GXNFW MCJKX IDDRU OPJQQ ZRHCN VWDYQ RDGDG
BXDBN PXFPU YXNFG MPJEL SANCD SEZZG IBEYU KDHCA MBJJF
KILCJ MFDZT CTJRD MIYZQ ACJRR SBGZN QYAHQ VEDCQ LXNCL
LVVCS QWBII IVJRN WNBRI VPJEL TAGDN IRGQP ATYEW CBYZT
EVGQU VPYHL LRZNQ XINBA IKWJQ RDZYF KWFZL GWFJQ QWJYQ
IBWRX
```

2. Consider a cryptosystem with key space $\mathcal{K}$, message space $\mathcal{M}$, and ciphertext space $\mathcal{C}$ that provides perfect secrecy. Assume that $p(C) > 0$ for all $C \in \mathcal{C}$.

   (a) [5 points] Prove that for any ciphertext $C \in \mathcal{C}$, there exists at least one key $K \in \mathcal{K}$ that encrypts some plaintext to C. Conclude that $|\mathcal{K}| \geq |\mathcal{C}|$.

   (b) [5 points] Conclude that if $|\mathcal{K}| \leq |\mathcal{M}|$, then $|\mathcal{K}| = |\mathcal{M}| = |\mathcal{C}|$ and all encryptions are bijections.

   (c) [6 points] Show that under the condition of part (b) every ciphertext is equally probable, i.e. $p(C) = 1/|\mathcal{C}|$ for all $C \in \mathcal{C}$.
   (*Hint:* Let $C \in \mathcal{C}$ be any ciphertext. se the statement on the uniqueness of keys in Shannon's Theorem to show that the function $g_C : \mathcal{K} \to \mathcal{M}$ via $g_C(K) = D_K(C)$ is a bijection. Now use the other statement in Shannon's Theorem, i.e. that every key is used with equal likelihood.)

3. [8 points] Use the characterization $p(C) = p(C|M)$ for all $C \in \mathcal{C}$ and $M \in \mathcal{M}$ to prove that one-time pad provides perfect secrecy under the assumption that each key is chosen with equal likelihood. Can you say anything about the distribution of ciphertexts?

4. For a bit string $\mathbf{x} \in \mathbb{Z}_2^n$, denote by $\overline{\mathbf{x}}$ the *ones' complement* of $\mathbf{x}$; that is, the i-th bit of $\overline{\mathbf{x}}$ is a '1' if and only if the i-th bit of $\mathbf{x}$ is a '0' for $1 \leq i \leq n$. Note that $\overline{\mathbf{x}} = \mathbf{1} \oplus \mathbf{x}$ where $\mathbf{1} \in \mathbb{Z}_2^n$ is the string consisting of n ones.

   (a) [4 points] Let M be a DES plaintext and K a DES key. Suppose $C = E_K(M)$ where E_M denote DES encryption under key K. Show that $\overline{C} = E_{\overline{K}}(\overline{M})$.

(b) [4 points] Suppose a cryptanalyst knows two plaintext-ciphertext pairs (M_1, C_1) and (M_2, C_2) with $C_i = E_K(M_i)$ $(i = 1, 2)$ for some DES key K (i.e. the same key is used for both encryptions) and $M_2 = \overline{M_1}$ (this scenario amounts to a CTA). How and by how much can this information reduce the effort of an exhaustive key search attack on DES? Explain.

5. In a cryptographic system, one wishes to avoid keys that provide a poor level of encryption; the worst scenario would obviously be $E_K(M) = M$ for all plaintexts M, but other keys have less drastic weaknesses.

   Two DES keys K_1 and K_2 are *dual* or *semi-weak* if $E_{K_1}(M) = D_{K_2}(M)$ for every $M \in \mathbb{Z}_2^{64}$. Such keys are obviously a disaster for double encryption as $E_{K_2}(E_{K_1}(M)) = M$ for all plaintexts M. If in addition, $K_1 = K_2$ $(= K$ say), i.e. $D_K = E_K$, then K is called *self-dual* or *palindromic*[1] or simply *weak*.

   (a) [4 points] Let C_0 be the left half and D_0 be the right half of the image of the relevant 56 bits of a DES key K under DES Permuted Choice PC-1. If C_0 is either all 0's or all 1's and D_0 is either all 0's or all 1's, then K is self-dual. Prove this in the case $C_0 = D_0 = 0^{56}$ (the other three cases can be proved analogously).

   (b) [4 points] The following four DES keys (given in hexadecimal, i.e. base 16, notation) are self-dual. Prove this fact for the first of these four keys (again, the proof for the other three is analogous).

```
0101 0101 0101 0101
FEFE FEFE FEFE FEFE
1F1F 1F1F 0E0E 0E0E
E0E0 E0E0 F1F1 F1F1
```

   It turns out that these are the only weak keys. It is a fact that each such key K has 2^{32} *fixed points*, i.e. plaintexts M for which $E_K(M) = M$.

   (c) [4 points] Let C_0 and D_0 be as in part (a). Prove that $C_0 = 0101\ldots01$ (in binary), then $C_i \oplus C_{17-i} = 1111\ldots11$ for $1 \le i \le 16$. State an analogous property for the D_i's.

   (d) [4 points] The following pairs of keys (given in hexadecimal notation) are dual:

```
01FE 01FE 01FE 01FE      FE01 FE01 FE01 FE01
1FE0 1FE0 0EF1 0EF1      E01F E01F F10E F10E
01E0 01E0 01F1 01F1      E001 E001 F101 F101
1FFE 1FFE 0EFE 0EFE      FE1F FE1F FE0E FE0E
011F 011F 010E 010E      1F01 1F01 0E01 0E01
E0FE E0FE F1FE F1FE      FEE0 FEE0 FEF1 FEF1
```

   Prove this for the first of these six pairs of keys (again, one can give analogous proofs for the other five). These are the only semi-weak keys.

   In practice, it is obviously easy to avoid the 16 keys listed above.

[1] A *palindrome* is a sequence of symbols that reads the same forwards as backwards, for example *"never odd or even"* or *"able was I ere I saw elba"*