# PMAT 669 Public Key Cryptography
# Assignment 1

Set: Sept. 26, 2005 Due: Oct. 12, 2005

(2) 1. Prove that for $n = 2, H(P)$ is maximal for $p_1 = p_2 = 1/2$.

(4) 2. Prove that for any $n, H(P)$ is maximal for $p_i = 1/n \, (i = 1, \ldots, n)$.

(3) 3. Why is a coherent running key cipher insecure?

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

(2) (a) Let $p$ be a DES plaintext and $k$ a DES key. Suppose $c = E_k(p)$ where $E_k$ denote DES encryption under key $k$. Show that $\overline{c} = E_{\overline{k}}(\overline{p})$.

(2) (b) Suppose a cryptanalyst knows two plaintext-ciphertext pairs $(p_1, c_1)$ and $(p_2, c_2)$ with $p_2 = \overline{p_1}$. How and by how much can this information reduce the effort of an exhaustive key search CPA on DES.

/over

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

Two DES keys $k_1$ and $k_2$ are *dual* or *semi-weak* if $E_{k_1}(x) = D_{k_2}(x)$ for every $x \in Z_2^{64}$. Such keys are obviously a disaster for double encryption as $E_{k_2}(E_{k_1}(x)) = x$ for all plaintexts $x$. If in addition, $k_1 = k_2 \, (= k \text{ say})$, i.e. $D_k = E_k$, then $k$ is called *self-dual* or *palindromic** or simply *weak*.

(2) (a) 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. Prove that 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.

(2) (b) Prove that the following four DES keys (given in hexadecimal, i.e. base 16, notation) are self-dual.

| | | | |
|---|---|---|---|
| 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 $p$ for which $E_k(p) = p$.

(3) 6. Show that in Rijndael, $\text{InvSubBytes}(\text{SubBytes}(a)) = a$ for all bytes $a$.

*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".