**Homework 1 (Due 09/19 )**

**Name:**

1. A substitution cipher replaces each letter with the one at the *i*-slots to its right.

| Position | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Letter | A | B | C | D | E | F | G | H | I | J | K | L | M |
| Position | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |
| Letter | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |

The key is “DAWN” and the ciphertext is “vealruwgwwk”. What is the original message? Please show the decryption process briefly.

1. DES is a 64-bit block cipher. Can two different keys encrypt a plaintext block into the same ciphertext block? If so, on average, how many DES keys can encrypt a particular plaintext block into a particular ciphertext block?
2. Assume the performance of a cryptographic algorithm for the good guys (the ones that know the key) grows linearly with the length of the key. The 128-bit key size is adequate in terms of performance (e.g., it can encrypt and decrypt as fast as the bits can be transmitted over the wire) and security (assume the only way to break it is key exhaustive search).

Now suppose the advances in computer technology make computers twice as fast, which means both good guys and bad guys get faster computers. Does this advance in computer speed work to the advantage of the good guys or the bad guys? Or it does not make any difference. Please explain your answer briefly.

1. A nonlinear function, such as S-Boxes in DES, is critical to the security of a block cipher. Without the nonlinear component, the block ciphers are vulnerable to linear analysis. Consider a linear block cipher c=**EL**(k, m), which encrypts 128-bit message block m into a 128-bit ciphertext block c using k-bit key k. **EL** cipher has a property as **EL**(k, m1⊕m2)=**EL**(k, m1) ⊕ **EL**(k, m2). This **EL** cipher is vulnerable to a chosen-ciphertext attack: with 128 chosen ciphertexts, an attacker can decrypt any ciphertext without knowing the k. Please explain how the attack works.