國立雲林科技大學 115 學年度 碩士班招生考試試題

系所：電子系

科目：計算機概論(3)

本試題共 8 題，每題得分如各題中所示，共計 100 分，請依題號作答並將答案寫在答案卷上，違者不予計分。

1. (10 pt.) Add the following bit patterns. Leave your results in binary form.

(a) 1011 + 0001

(b) 0000 + 1010

(c) 1100 + 0011

(d) 0101 + 0110

(e) 1111 + 0001

2. (10 pt.) Convert these decimal numbers to 8-bit 2's complement binary numbers.

(a) 102

(b) 64

(c) 33

(d) -128

(e) 127

3. (20 pt.) If the Y is output and A, B is input, the XOR function can be shown as follows:

$$Y = \overline{A}B + A\overline{B}$$

Implement the XOR function by means of :

(a) (10 pt.) NAND gates only.

(b) (10 pt.) NOR gates only.

4. (10 pt.) Implement a 4-to-1 mux using only 2-to-1 mux making sure to properly connected all of the terminals. Remember that you will have 4 inputs, 2 control signals, and 1 output. Write out the truth table for this circuit.

5.(10 pt.) The following list contains several types of memory and storage devices commonly used in computer systems:

- CPU Register
- Cache Memory
- DDR5 Main Memory (RAM)
- SSD (Solid-State Drive)
- HDD (Hard Disk Drive)
- ROM (Read-Only Memory)

Questions

1. (6 pt.)Classify each item above as either Volatile Memory or Non-Volatile Memory.
2. (2 pt.)Among all the items listed, which one has the fastest access speed?
3. (2 pt.)Among all the items listed, which one has the slowest access speed?

6. (10 pt.) According to the IEEE 754 single-precision (32-bit) floating-point standard, a number is represented in hexadecimal as:

$$0xC2480000_{(16)}$$

Questions

1. (5 pt.)Identify the sign bit, exponent field, and fraction (mantissa).
2. (5 pt.)Determine the decimal value represented by this IEEE 754 single-precision floating-point number.

7. (15 pt.) Alice and Bob communicate over a public network. Before transmitting messages, they first apply the Diffie–Hellman (DH) key exchange algorithm to generate a shared secret key, which is then used to encrypt the message using the XOR operation. This mechanism ensures that even if the communication is intercepted, the original plaintext cannot be directly recovered.
The public parameters for the Diffie–Hellman algorithm are given as:

- Generator: g=5
- Prime modulus: p=23

Alice and Bob independently choose their private keys:

- Alice's private key: a=2 (known only to Alice)
- Bob's private key: b=4 (known only to Bob)

Alice sends the following ciphertext words to Bob (all values are 16-bit and represented in hexadecimal):

0x58, 0x59, 0x31, 0x31

國立雲林科技大學 115 學年度 碩士班招生考試試題

系所：電子系

科目：計算機概論(3)

Questions

1. (7 pt.)Compute the public values A and B, and determine the shared secret key K.
2. (8 pt.)Determine the decrypted plaintext words P1, P2, P3, and P4.

8. (15 pt.) Alice and Bob communicate confidential experimental data through a public network. To secure the transmission, they decide to use the RSA cryptosystem. They select two prime numbers p=7 and q=17 to construct their RSA keys.

1. Let $N=p\times q$.
2. Choose the smallest integer greater than 10 that is coprime with $(p-1)(q-1)$ as the public exponent eee.
3. Bob's private key exponent ddd is chosen such that

$$e\times d \equiv 1 (\text{mod } (p-1)\ (q-1))$$

and d lies in the range 40 to 60.

Question:

Determine

1. (5 pt.) Alice's public key (e, N)
2. (10 pt.) Bob's private key (d, N)