NATIONAL UNIVERSITY OF SINGAPORE

**SCHOOL OF COMPUTING**

**SEMESTER II AY2017/2018**

Deleted:

# FINAL ASSESSMENT FOR
# CG1112: ENGINEERING PRINCIPLES AND PRACTICE II

21st April 2018 Time Allowed: 1 Hour

## INSTRUCTIONS TO CANDIDATES:

1. Use **2B Pencil** to shade the **OCR form**. Ensure your student number is shaded properly.
2. This assessment paper consists of **FIFTEEN (15)** questions.
3. This assessment paper comprises **SEVEN ( 7 ) printed pages** including this front page.
4. Each MCQ carries 1 mark. No penalty for wrong answer. Total marks for the paper is **15**.
5. This is a **close book assessment** with **one A4 reference sheet** allowed.
6. Submit only the **OCR** form at the end of the assessment.

1. Dinah just implemented his own new hash function to be used in TLS encryption system. The hash function takes a message of arbitrary length and produce a 256-byte **digest**. As a test, he produce a digest **D** from a message **M** of 4096 bytes. His good friend Eve found that she can find another message **M'** that differs from **M**, but still result in the same digest **D**. Which properties is/are lacking from Dinah's hash function?

    i. Non-Trivial
    ii. Sensitive to input change
    iii. Irreversible

    a. i only
    b. ii only
    c. i and iii only
    d. ii and iii only
    e. i, ii and iii

Comment [ys1]: Answer.

2. The TLS certificate of a website is publicly available (i.e., requester can just send a request and receive a copy of the certificate from the website). Alice thought that she can make the website more secure by **encrypting the certificate using the requester's public key before sending it out**. This should prevent any 3rd party to get a copy of the website certificate. Which of the following statement is the most accurate evaluation of this idea?

    a. **Alice is right**: the certificate cannot be easily duplicated by 3rd party now.
    b. **Alice is right**: the attacker cannot request for certificate.
    c. **Alice is wrong**: the requester will not be able to decrypt the certificate.
    d. **Alice is wrong**: there is no easy way to get the public key of the requester.
    e. **Alice is wrong**: the attacker can just request for certificate.

Deleted: TLC

Deleted:

Formatted: Highlight

Comment [ys3]: Answer

3. Suppose we use **bare-metal programming** to send out an array of **64 integers** from Atmega328p. How many times do we need to assign (place a value) in the UDR0 (USART Data Register) for transmitting the entire array using **polling-** and **interrupt-**based code?

| | **Polling** | **Interrupt** |
|---|---|---|
| a. | 64 | 64 |
| b. | 128 | 128 |
| c. | 256 | 64 |
| d. | 128 | 64 |
| e. | 64 | 128 |

Comment [ys4]: Ans

4. Suppose each of the RPLidar scan data (each point) takes **4 bytes**, what is the minimum bandwidth for the serial communication between the RPLidar and Pi if the lidar is operating at the optimum 10 Hz scanning speed?

Formatted: English (UK)

a. 320 bps (bits per second)
b. 1,440 bps
c. 14,400 bps
d. 115,200 bps
e. None of the above

Comment [ys5]: 360 data points per round x 10 rounds x 4 bytes x 8 bits

5. Which of the following regarding the **Hector SLAM** used in our project is / are correct?
   i. Hector SLAM estimates its movement by using the compass / magnetometer
   ii. Hector SLAM does not use odometry data from the motor
   iii. Hector SLAM differs from other SLAM algorithms as it does not try to re-observe landmarks.

a. i only
b. ii only
c. i and iii only
d. ii and iii only
e. i, ii and iii

Comment [ys6]: Answer

6. The AT328P that you are currently using in your EPP2 lab has a built-in ADC module. Refer to the following statements with reference to your AT328p microcontroller. Which statement is TRUE?

   a. It has 6 ADC modules with 6 ADC input channels
   b. It has 8 ADC modules with 8 ADC input channels
   c. It has 1 ADC module with 6 ADC input channels
   d. It has 1 ADC module with 8 ADC input channels
   e. It has 1 ADC module with 1 ADC channel

Comment [TKYC7]: Answer

Deleted: .

7. An input signal in the range of 0 – 0.6 V is supplied to the ADC module of the AT328p microcontroller. What is the largest ADC value (rounded-up) you can expect from it?

   a. 600
   b. 488
   c. 321
   d. 123
   e. 1024

Deleted:

Comment [TKYC8]: Answer

8. Further to questions 6 and 7, what is the gain that is necessary in order for the input signal to be mapped to the full input range of the ADC module in the AT328p.

   a. 8.33
   b. 6.0
   c. 10
   d. 0.12
   e. 1.5

Deleted: What

Comment [TKYC10]: Answer

9. The correct gain is provided and the ADC operation is then performed. The ADC result is 0b0011111010. What is the actual voltage of the signal (correct to 2 decimal place)?

   a. 0.24 V
   b. 1.22 V
   c. 1.23 V
   d. 0.15 V
   e. 1.23 V

Comment [TKYC11]: Answer

10. You decide to operate Timer0 in Fast PWM mode. The WGM0[2:0] bits are set to 0x3. What is the frequency of the PWM signal with the prescaler set to 1.

| Mode | WGM02 | WGM01 | WGM00 | Timer/Counter Mode of Operation | TOP | Update of OCR0x at | TOV Flag Set on[1][2] |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | Normal | 0xFF | Immediate | MAX |
| 1 | 0 | 0 | 1 | PWM, Phase Correct | 0xFF | TOP | BOTTOM |
| 2 | 0 | 1 | 0 | CTC | OCRA | Immediate | MAX |
| 3 | 0 | 1 | 1 | Fast PWM | 0xFF | BOTTOM | MAX |
| 4 | 1 | 0 | 0 | Reserved | - | - | - |
| 5 | 1 | 0 | 1 | PWM, Phase Correct | OCRA | TOP | BOTTOM |
| 6 | 1 | 1 | 0 | Reserved | - | - | - |
| 7 | 1 | 1 | 1 | Fast PWM | OCRA | BOTTOM | TOP |

a. 3 kHz
b. 256 kHz
c. 128 kHz
d. 62.5 kHz
e. 31.25 kHz

**Comment [TKYC12]:** Answer

11. The TLS client-server programs used in Vincent aren't very secure; this is because:

a. The symmetric encryption used is weak.
b. The key exchange mechanism used is weak and the secret key can be derived, though with some effort, from the information exchanged between TLS hosts.
c. The TLS server on Vincent does not check the client's certificates.
d. We only use 2048-bit keys, which is too small.
e. The asymmetric cipher used is not secure.

**Comment [CT13]:** a. is false. TLS algorithms are constantly audited by security professionals and weak algorithms are taken out of use (e.g. SSLv2 and SSLv3)
b.is false. Algorithms like Diffie-Hellman require knowledge of secret information to derive the keys. The keys cannot be extracted from the information exchanged.
c.is TRUE, while the client verifies the robot's Pi, the Pi does not verify the client, which means any client can connect to Vincent and control him.
d.2048 bit RSA is industry standard and it means that an attacker must search a space of 2^2048 integers to try to crack a key, which takes very long.
e.RSA is known to be secure, or it would not be in use today.
ANSWER: C

12. Alice has the following data structure:

```
typedef struct t
{
      int x;
      char str[6];
      float y;
} TData;

TData data;
```

She populates "data" in her code then serializes it using:

```
char buffer[255];
memcpy(buffer, &data, sizeof(TData));
```

And sends it out, together with length information, to Bob over a highly reliable channel that delivers packets without any loss or corruption. When Bob gets the message he de-serializes with:

```
char buffer[128];

recvData(buffer); // Actually receive data sent by Alice.
TData data;
memcpy(&data, buffer, sizeof(TData));
```

Unfortunately the data he gets is garbled. Which of the following is **NOT** a possible cause for the data becoming garbled?

a. The integer and/or floating-point widths used in Alice's and Bob's machines are different.
b. The byte ordering between Alice's and Bob's machines are different.
c. Bob uses a buffer that is too small (128 bytes vs. Alice's 255 bytes).
d. The compilers used in Alice's and Bob's machines are padding in different number of bytes to the data structures.
e. All of the options above a. to d. are possible causes for the data becoming garbled.

**Comment [CT14]:**

**Formatted:** Font:Bold

**Comment [CT15]:** a.YES: Differing int widths can cause errors as explained in the lecture.
b.YES: Differing endianness can cause a program to accidentally reverse the data.
c. NO: As long as the buffer is large enough to hold the data structure (between 9 to 17 bytes here), the buffer size does not matter.
d. YES: E.g. we saw that the Arduino does not pad anything to the char, but the Pi pads in 3 bytes.
e.Since c. is NO, this cannot be right.
Answer: C

**Comment [SWS16]:** Just say none of the above?

13. Which of the following statements about serial communications is FALSE?

a. Parity checks cannot detect an even number of bit errors in a byte.
b. The receiver and transmitter must have the same baud-rate and frame format before they can communicate with each other.
c. The transmitter must send clocking information to the receiver before transmission begins.
d. The serial line is normally held in a logical HIGH state, but is pulled low just prior to sending the first bit.
e. In Atmega328P sending in double-speed mode can result in more data being incorrectly received due to poor built system clocks.

**Comment [CT17]:** a.TRUE: E.g. in 7E1, one bit error will make the # of 1 bits odd, but a second will make it even again, making it impossible to detect the error.
b.TRUE, both sides must agree on baud rate, format (e.g. 8N1), and though not mentioned much, also in terms of flow control.
c.FALSE: The receiver derives the clocking information directly from the signal.
d.TRUE: This low is the START bit.
e.TRUE: Double-speed mode requires stable clocking circuits to ensure correctness.

Answer: c

14. Given a transmission rate of 9600 baud in 8N1 format, what is the fastest rate at which you can write to UDR0 without causing loss of data? Choose the best available answer.

a. One character every 0.83 ms.
b. One character every 1.04 ms.
c. One character every 1.83 ms
d. One character every 2.08 ms
e. One character every 2.85 ms

**Comment [CT18]:** Every character has a start bit and a stop bit, giving 10 bits per character. Thus 9600 bps is equivalent to 960 cps, and 1/960 gives us just under 1.1ms between characters. So answer is b.

Answer: b

**Comment [SWS19R18]:** Maybe give two decimal places?

**Deleted:** 8

**Deleted:** 1

**Deleted:** 2

15. Which ONE of the following statements about TCP/IP is FALSE?

a. IP packets sent in sequence from the source can arrive out of sequence at the destination.
b. IP packets that are sent out may never arrive at the destination.
c. Two IP packets bound for the same destination may travel over two completely different routes.
d. If we receive “Request timeout” when we ping a host, it means that the host is down.
e. TCP ensures that the socket application receives packets in the correct order.

**Comment [CT20]:** a.TRUE, because packets take different routes with different latencies.
b.TRUE. IP is best effort, and packets may be dropped at routers for various reasons.
c.TRUE, reason also why a. is true.
d.FALSE. The destination host may be configured to drop ICMP packets and thus never respond to the pings.
e.TRUE. TCP re-orders packets to ensure they are joined back in the correct order.

**Deleted:**