# 50.042 Foundations of Cybersecurity
# Final Exam Practice Questions

**Multiple Choice Questions**

Circle the correct answer. There is only **one** correct answer for each question, unless stated otherwise.

1. (Certificate authority) Which of the following is **true**, with regards to a certificate authority (CA)?
    a. The CA **always** generates a public and private key pair on behalf of the user
    b. The CA signs the user's **private** key, using its own **public** key and a digital signature protocol
    c. The CA generates the user's **private** key, using its own **public** key and a key establishment protocol
    d. The CA signs the user's **public** key, using its own **private** key and a digital signature protocol

2. (Digital signatures) Which key is used to **sign** the plaintext message in a digital signature scheme?
    a. The sender's **public** key
    b. The sender's **private** key
    c. The receiver's **public** key
    d. The receiver's **private** key

decrypt

3. (Symmetric ciphers) Which of the following is **not** a **symmetric** key algorithm?
   a. AES
   b. RSA
   c. OTP
   d. DES

4. (Modular arithmetic) Which one of the following statements is **true**?
   a. $\mathbb{Z}^*_{10}$ is not a group
   b. The order of $\mathbb{Z}^*_{13}$ is 13
   c. $\mathbb{Z}^*_{7}$ is not a cyclic group
   d. $\mathbb{Z}^*_{19}$ contains an element that is a generator

every prime group has generator

prime

(Simplified Bell-LaPadula model) Use the information and tables below for **questions 5 and 6**.

- Security clearances: **SL** (lower), **AM** (higher)
- Integrity clearances: **ISL** (lowest). **IO** (middle), **ISP** (highest)
- **SP**, **SD** and **SSD** are security categories
- **IP** and **ID** are integrity categories

| Subject | Security Level (simplified) | Integrity Level |
|---|---|---|
| Ordinary users | (SL, {SP}) | (ISL, {IP}) |
| Application developers | (SL, {SD}) | (ISL, {ID}) |
| System managers | (AM, {SP, SD, SSD}) | (ISL, {IP, ID}) |

Read write

| Object | Security Level (simplified) | Integrity Level |
|---|---|---|
| Development code / test data | (SL, {SD}) | (ISL, {ID}) |
| Production code | (SL, {SP}) | (IO, {IP}) |
| Production data | (SL, {SP}) | (ISL, {IP}) |
| System programs | (SL, Ø) | (ISP, {IP, ID}) |
| System programs under modification | (SL, {SSD}) | (ISL, {ID}) |

5. (Simplified Bell-LaPadula model) Which of the following statements is **true** for **system managers**?
   a. They have both read and write access to system programs → R only.
   b. They have only write access to production data → R & W
   c. They have only read access to system programs → R only
   d. They have only read access to development code → R & W

6. (Simplified Bell-LaPadula model) Which of the following statements is **true** for **production code**?

   ~~a.~~ They can be written by system managers
   ~~b.~~ They can be written by ordinary users
   c. They can be read by system managers
   ~~d.~~ They can be read by application developers

## Long answer questions

1. (Modular arithmetic) This question consists of two sections: Parts a) and b).

   a) Compute $7^{25}$ *mod* 52 using the square and multiply algorithm. Show your work.

$x = 7$

$25_{10} = 11001_2 \rightarrow$ 4 iters

$1^{st}$ iter $\rightarrow$ bit = '1'

$7^2 \bmod 52 \times x$

$= 49 \bmod 52 \times 7$

$= 31 \bmod 52$

$2^{nd}$ iter $\rightarrow$ bit = '0'

$31^2 \bmod 52$

$= 961 \bmod 52$

$= 25 \bmod 52$

$3^{rd}$ iter $\rightarrow$ bit '0'

$25^2 \bmod 52$

$= 625 \bmod 52$

$= 1 \bmod 52$

$4^{th}$ iter $\rightarrow$ bit '1'

$1^2 \bmod 52 \times 7$

$= 7 \bmod 52$

$7^{25} \bmod 52 \equiv 7 \bmod 52$

b) Find the order of the following elements, given their respective groups.

i. Element: 5
Group: $\mathbb{Z}^*_8$

find smallest $5^k$ st $5^k \bmod 8 \equiv 1 \bmod 8$

$5^1 \bmod 8 = 5$

$5^2 \bmod 8 = 25 \bmod 8 = 1 \bmod 8$

order of 5 in $\mathbb{Z}^*_8 = 2$.

ii. Element: 9
Group: $\mathbb{Z}^*_{11}$

$9^1 \bmod 11 = 9 \bmod 11$

$9^2 \bmod 11 = 81 \bmod 11$
$= \boxed{4 \bmod 11}$

$9^3 \bmod 11 = \boxed{4 \bmod 11} \times 9$
$= 36 \bmod 11 = \boxed{3 \bmod 11}$

$9^4 \bmod 11 = \boxed{3 \bmod 11} \times 9$
$= 27 \bmod 11 = \boxed{5 \bmod 11}$

$9^5 \bmod 11 = \boxed{5 \bmod 11} \times 9$
$= 45 \bmod 11 = 1 \bmod 11$

2. (Information flow and entropy) Suppose we have the following code segment:

```
x = w - z
k = z + y[i]
```

From our lectures, we know that with respect to the **first line** of the code segment, there is information flow **from** the variables **`w`** and **`z`** **to** the variable **`x`**.

a) Let *I*, *K*, *W*, *X*, *Y[I]* and *Z* be **random variables** representing the variables **`i`**, **`k`**, **`w`**, **`x`**, **`y[i]`** and **`z`** respectively in the code segment above.
Also, let $\underline{I}$, $\underline{K}$, $\underline{W}$, $\underline{X}$, $\underline{Y[I]}$ and $\underline{Z}$ represent the **security classes** of *I*, *K*, *W*, *X*, *Y[I]* and *Z* respectively.

Write an expression (in terms of $\underline{I}$, $\underline{K}$, $\underline{W}$, $\underline{X}$, $\underline{Y[I]}$ and $\underline{Z}$) that must be stated in the **security policy** for a **compiler-based mechanism**, in order for the above code segment to be **certified**.

$\max(W, Z) \leq X$ , $\max(Z, I, Y[I]) \leq K$

or $W \leq X$ , $Z \leq X$ , $Z \leq K$, $I \leq K$ , $Y[I] \leq K$.

(more parts to this question on the next page)

In the subsequent parts of this question, we will focus only on the **first line** of the above code segment. We will show that there is information flow from the variable **w** to the variable **x**.

For the rest of this question, let $X$, $W$ and $Z$ be **discrete random variables** representing the variables **x**, **w** and **z** respectively in the code segment above. Assume that **state *a*** represents the state **before** the above code segment is executed, while **state *b*** represents the state **after** the above code segment is executed.

Note the following important points:

- $W_a$ is distributed between the set of **integer** values {2, 3}, with the following probabilities:

| $P(W_a = 2)$ | $P(W_a = 3)$ |
|---|---|
| $\frac{2}{3}$ | $\frac{1}{3}$ |

$\frac{1}{3}$ $\frac{1}{3}$ $\frac{1}{3}$

- $Z_a$ is distributed **equally** between the set of **integer** values {0, 1, 2}

- $X$ does **not** exist in state $a$. This means that $X_a$ does **not** exist.

b) Based on the above code segment, $X$ can be one of four integer values in state $b$: 0, 1, 2 or 3. Calculate the probabilities of $X_b$ and fill in the table below. Leave your answers as fractions or as numbers rounded to 3 decimal places. Show your work.

$x = w - z$ $w=2 : \frac{2}{3}$ $z=0 : \frac{1}{3}$

$w=3 : \frac{1}{3}$ $z=1 : \frac{1}{3}$

$z=2 : \frac{1}{3}$

$2-2$ $2-1$ $\frac{2}{9}$ $2-0 : \frac{2}{9}$ $3-0 : \frac{1}{9}$

$3-2$ $\frac{1}{9}$ $3-1 : \frac{1}{9}$

| $P(X_b = 0)$ | $P(X_b = 1)$ | $P(X_b = 2)$ | $P(X_b = 3)$ |
|---|---|---|---|
| $\frac{2}{9}$ | $\frac{1}{3}$ | $\frac{1}{3}$ | $\frac{1}{9}$ |

(more parts to this question on the next page)

$P(w=2) = \frac{2}{3}$ $P(w=3) = \frac{1}{3}$

c) Calculate the value of H($W_a$), i.e. the entropy of $W_a$. Leave your answer as a number rounded to 3 decimal places. Show your work.

$$H(W_a) = -\sum_{i=1}^{2} P(W_a = w_i) \cdot \log_2 P(W_a = w_i)$$

$$= -\left[P(w=2) \cdot \log_2 P(w=2) + P(w=3) \cdot \log_2 P(w=3)\right]$$

$$= -\left[\frac{2}{3} \cdot \log_2 \left(\frac{2}{3}\right) + \frac{1}{3} \log \left(\frac{1}{3}\right)\right]$$

$$= 0.918.$$

(more parts to this question on the next page)

$x=0 \Rightarrow \frac{2}{9}$ $z=0: \frac{1}{3}$

$w=2 \Rightarrow \frac{2}{3}$ $x=1 \Rightarrow \frac{1}{3}$ $z=1: \frac{1}{3}$

$x=2 \Rightarrow \frac{1}{3}$

$w=3 \Rightarrow \frac{1}{3}$ $x=3 \Rightarrow \frac{1}{9}$ $z=2: \frac{1}{3}$

d) Calculate the various **conditional** probabilities of $W_a$ with respect to $X_b$ and fill in the table below. Leave your answers as fractions or as numbers rounded to 3 decimal places. Show your work.

*Hint: use Baye's Theorem.*

$$P(W_a = 2 \mid X_b = 0) = \frac{P(X_b = 0 \mid W_a = 2) \cdot P(W_a = 2)}{P(X_b = 0)} = \frac{\frac{1}{3} \cdot \frac{2}{3}}{\frac{2}{9}} = 1$$

$$P(W_a = 3 \mid X_b = 0) = \frac{P(X_b = 0 \mid W_a = 3) \cdot P(W_a = 3)}{P(X_b = 0)} = \frac{0 \cdot \frac{1}{3}}{\frac{2}{9}} = 0$$

$$P(W_a = 2 \mid X_b = 1) = \frac{P(X_b = 1 \mid W_a = 2) \cdot P(W_a = 2)}{P(X_b = 1)} = \frac{\frac{1}{3} \cdot \frac{2}{3}}{\frac{1}{3}} = \frac{2}{3}$$

$$P(W_a = 3 \mid X_b = 1) = \frac{P(X_b = 1 \mid W_a = 3) \cdot P(W_a = 3)}{P(X_b = 1)} = \frac{\frac{1}{3} \cdot \frac{1}{3}}{\frac{1}{3}} = \frac{1}{3}$$

$$P(W_a = 2 \mid X_b = 2) = \frac{P(X_b = 2 \mid W_a = 2) \cdot P(W_a = 2)}{P(X_b = 2)} = \frac{\frac{1}{3} \cdot \frac{2}{3}}{\frac{1}{3}} = \frac{2}{3}$$

$$P(W_a = 3 \mid X_b = 2) = \frac{P(X_b = 2 \mid W_a = 3) \cdot P(W_a = 3)}{P(X_b = 2)} = \frac{\frac{1}{3} \cdot \frac{1}{3}}{\frac{1}{3}} = \frac{1}{3}$$

$$P(W_a = 2 \mid X_b = 3) = \frac{P(X_b = 3 \mid W_a = 2) \cdot P(W_a = 2)}{P(X_b = 3)} = \frac{0 \cdot \frac{2}{3}}{\frac{1}{9}} = 0$$

$$P(W_a = 3 \mid X_b = 3) = \frac{P(X_b = 3 \mid W_a = 3) \cdot P(W_a = 3)}{P(X_b = 3)} = \frac{\frac{1}{3} \cdot \frac{1}{3}}{\frac{1}{9}} = 1$$

| $P(W_a = 2 \mid X_b = 0)$ | $P(W_a = 2 \mid X_b = 1)$ | $P(W_a = 2 \mid X_b = 2)$ | $P(W_a = 2 \mid X_b = 3)$ |
|---|---|---|---|
| 1 | $\frac{2}{3}$ | $\frac{2}{3}$ | 0 |
| $P(W_a = 3 \mid X_b = 0)$ | $P(W_a = 3 \mid X_b = 1)$ | $P(W_a = 3 \mid X_b = 2)$ | $P(W_a = 3 \mid X_b = 3)$ |
| 0 | $\frac{1}{3}$ | $\frac{1}{3}$ | 1 |

(more parts to this question on the next page)

e) Calculate the value of H($W_a$ | $X_b$), i.e. the **conditional** entropy of $W_a$ given $X_b$. Leave your answer as a number rounded to 3 decimal places. **Verify** that information flows from $W$ to $X$, by comparing the value of H($W_a$ | $X_b$) with the value of H($W_a$) you obtained in part c). Show your work.

$$\mathbf{H}(Y_a \mid X_b) = -\sum_{j=1}^{4} \mathbf{P}(X_b = x_j) \cdot \sum_{i=1}^{2} \mathbf{P}(W_a = w_i \mid X_b = x_j) \cdot \log_2 \mathbf{P}(W_a = w_i \mid X_b = x_j)$$

Thus, $\mathbf{H}(W_a \mid X_b) =$

$$-\mathbf{P}(X_b = 0) \cdot [\mathbf{P}(W_a = 2 \mid X_b = 0) \cdot \log_2 \mathbf{P}(W_a = 2 \mid X_b = 0) + \mathbf{P}(Y = W_a = 3 \mid X_b = 0) \cdot \log_2 \mathbf{P}(W_a = 3 \mid X_b = 0)]$$

$$-\mathbf{P}(X_b = 1) \cdot [\mathbf{P}(W_a = 2 \mid X_b = 1) \cdot \log_2 \mathbf{P}(W_a = 2 \mid X_b = 1) + \mathbf{P}(Y = W_a = 3 \mid X_b = 1) \cdot \log_2 \mathbf{P}(W_a = 3 \mid X_b = 1)]$$

$$-\mathbf{P}(X_b = 2) \cdot [\mathbf{P}(W_a = 2 \mid X_b = 2) \cdot \log_2 \mathbf{P}(W_a = 2 \mid X_b = 2) + \mathbf{P}(Y = W_a = 3 \mid X_b = 2) \cdot \log_2 \mathbf{P}(W_a = 3 \mid X_b = 2)]$$

$$-\mathbf{P}(X_b = 3) \cdot [\mathbf{P}(W_a = 2 \mid X_b = 3) \cdot \log_2 \mathbf{P}(W_a = 2 \mid X_b = 3) + \mathbf{P}(Y = W_a = 3 \mid X_b = 3) \cdot \log_2 \mathbf{P}(W_a = 3 \mid X_b = 3)]$$

$$= -\frac{2}{9}[1 \cdot \log_2 1 + 0 \cdot \log_2 0]$$

$$-\frac{1}{3}\left[\frac{2}{3} \cdot \log_2 \frac{2}{3} + \frac{1}{3} \cdot \log_2 \frac{1}{3}\right]$$

$$-\frac{1}{3}\left[\frac{2}{3} \cdot \log_2 \frac{2}{3} + \frac{1}{3} \cdot \log_2 \frac{1}{3}\right]$$

$$-\frac{1}{9}[0 \cdot \log_2 0 + 1 \cdot \log_2 1]$$

$$= 0.612$$

Since $\mathbf{H}(W_a) = 0.918$, we have $\mathbf{H}(W_a \mid X_b) < \mathbf{H}(W_a)$ and so information has flowed from $\boldsymbol{W}$ to $\boldsymbol{X}$.