Supposed you are logged in as user Alice, whose home directory is /home/alice, and the current directory is /home/alice/Documents/. Suppose you execute the following command:

$ cd ~/../bin/

Which one of the following statements best describes the effect of this command?

Question 1

Select one:

a.

It will change the current directory to the /bin, because the symbol ~ represents /home/ directory, so ~/../bin resolves to /bin.

b.

It will produce an error, because the path ~/../bin/ resolves to /bin, which does not exist.

c.

It will produce an error, because the path ~/../bin/ resolves to /home/bin, which does not exist.

d.

It will change the current directory to /root/bin/.

#### Feedback

Your answer is correct.

The correct answer is:

It will produce an error, because the path ~/../bin/ resolves to /home/bin, which does not exist.

### Question **2**

Incorrect

Mark 0.00 out of 0.50

Flag question

#### Question text

Suppose you are logged in as user 'Alice' and the home directory of Alice is /home/alice, and you execute the following commands:

$ export PATH=/usr/bin:/bin:/home/alice:/usr/local/bin  
$ cp /bin/echo ~/ls  
$ ls /etc

Which statement below best describes the effect of these commands?

Question 2

Select one:

a.

A string containing ’/etc’ is displayed, because the ‘ls’ command in the last line is actually the program ‘echo’.

b.

A string containing ‘/etc/‘ is displayed, because the command `ls’ always refers to /bin/ls irrespective of the value of the PATH environment variable.

c.

The content of the directory /etc/ is displayed.

d.

An error occurs because the user tries to override a system command.

#### Feedback

Your answer is incorrect.

The correct answer is: The content of the directory /etc/ is displayed.

### Question **3**

Correct

Mark 0.50 out of 0.50

Flag question

#### Question text

Suppose the current directory has two directories:

dir1   
dir2

and two files

doc1  
exe1

What does the following command do?

$ ls d?

Question 3

Select one:

a.

It will display a list containing 'doc1' and the contents of subdirectories dir1 and dir2.

b.

It will display a list containing only 'doc1'.

c.

It will display all files (but not directories) in the current directory.

d.

It will display the content of the file 'doc1'.

e.

It will display an error message.

#### Feedback

Your answer is correct.

The correct answer is: It will display an error message.

### Question **4**

Correct

Mark 1.00 out of 1.00

Flag question

#### Question text

Consider the following shell script:

#!/bin/bash  
read x  
if [ $x = $USER ]   
then   
 echo "Correct"  
else  
 echo "Wrong"  
fi

Which of the following statements best describes a behaviour of the above shell script?

Question 4

Select one:

a.

It reads a string from the standard input, outputs "Wrong" to the standard output if the input is the same as the username of the current user. Otherwise, it outputs "Correct".

b.

It reads a string from the standard input, outputs "Correct" to the standard output if the input is the same as the username of the current user. Otherwise, it outputs "Wrong".

c.

It always output "Wrong" no matter what input is provided to the script.

d.

It reads a string from the standard input, outputs "Correct" to the standard output if the input is the string "$USER".

#### Feedback

Your answer is correct.

The correct answer is: It reads a string from the standard input, outputs "Correct" to the standard output if the input is the same as the username of the current user. Otherwise, it outputs "Wrong".

### Question **5**

Correct

Mark 0.50 out of 0.50

Flag question

#### Question text

Which one of the following commands finds all the files and directories whose names start with ‘conf’ in the /etc directory?

Question 5

Select one:

a.

find /etc/ -name "conf"

b.

find /etc/ -name "conf\*"

c.

find /etc/ -name "\*conf"

d.

find -name "conf" /etc/

#### Feedback

Your answer is correct.

The correct answer is: find /etc/ -name "conf\*"

### Question **6**

Correct

Mark 1.00 out of 1.00

Flag question

#### Question text

Consider the following script:

#!/bin/bash  
i=1  
j=0  
while [ $i -lt 10 ]  
do  
 ((j=i+j))  
 ((i=i+1))  
done  
echo $j

This script is supposed to calculate the sum of the first 10 integers (1+2+…+10). There is a mistake in the script. Which of the following fixes this mistake?

Question 6

Select one:

a.

Replace ‘((j=i+j))’ with ‘((j=i+10))’

b.

Replace ‘((i=i+1))’ with ‘((i=i+2))’

c.

Replace ‘j=0’ with ‘j=1’

d.

Replace ‘while [ $i -lt 10 ]’ with ‘while [ $i -le 10 ]’

#### Feedback

Your answer is correct.

The correct answer is: Replace ‘while [ $i -lt 10 ]’ with ‘while [ $i -le 10 ]’

### Question **7**

Correct

Mark 1.00 out of 1.00

Flag question

#### Question text

Which command(s) below display the names of the first 15 files, alphabetically ordered, in directory /bin? Select all applicable answers.

Question 7

Select one or more:

a.

ls /bin > ~/list.txt | head -n ~/list.txt

b.

ls /bin; head -n 15

c.

ls /bin > ~/list.txt ; head -n 15 ~/list.txt

d.

ls /bin | head -n 15

e.

ls /bin | grep 15

f.

head -n 15 < ls /bin

#### Feedback

Your answer is correct.

The correct answers are: ls /bin > ~/list.txt ; head -n 15 ~/list.txt, ls /bin | head -n 15

What type of attacks does password salting prevent?

Question 1

Select one:

a.

Phishing attack

b.

Offline password guessing via pre-computed hash table

c.

Offline password guessing via dictionary attack

d.

Reuse of stolen password

#### Feedback

Your answer is correct.

The correct answer is: Offline password guessing via pre-computed hash table

### Question **2**

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

Assuming that every password is chosen with equal probability, which one of the following password policies gives the highest entropy?

Question 2

Select one:

a.

A password must be of length 8 and each character is a lower-case letter ranging from ‘a’ to ‘z’ or an upper-case letter ranging from ‘A’ – ‘Z’.

b.

A password must be of length 16 and each character is a lower-case letter ranging from ‘a’ to ‘z’.

c.

A password must be a 16-digit number.

d.

A password must be of length 8 and each character is a lower-case letter ranging from ‘a’ to ‘z’ or a number ranging from ‘0’ – ‘9’.

e.

A password must be of length 8 and each character is a lower-case letter ranging from ‘a’ to ‘z’ or an upper-case letter ranging from ‘A’ – ‘Z’ or a number ranging from ‘0’ – ‘9’.

#### Feedback

Your answer is correct.

The correct answer is: A password must be of length 16 and each character is a lower-case letter ranging from ‘a’ to ‘z’.

### Question **3**

Correct

Mark 1.00 out of 1.00

Flag question

#### Question text

Consider the following biometric authentication scheme implemented in a computer system: to log in to the system, a user, say Alice, types in her username and scans her fingerprint, and the system looks up the database of enrolled users to find the fingerprint registered under Alice’s username. If Alice’s username is registered and the scanned fingerprint matches with the reference fingerprint for Alice in the database, then the authentication succeeds; otherwise the system will reject the login attempt.

Suppose the system has 200 users registered, and Alice is among these users, and assume the fingerprint scanner has an FTA of 0.5%, FNMR of 2.8% and FMR of 2.5%. What is the probability that Alice fails to log in to the system?

Give your answer as a percentage, rounded up to two decimal places.

Answer:

Question 3

#### Feedback

This corresponds to FRR = FTA + (1-FTA)\*FNMR

The correct answer is: 3.29

In modern Linux systems, such as Ubuntu 20.04, user password hashes are stored in /etc/passwd file.

Question 1

Select one:

True

False

#### Feedback

In modern Linux systems, password hashes are stored in /etc/shadow, which can only be accessed by the root user. The /etc/passwd contains general user information but not the password hashes. This is because /etc/passwd is readable by all users in the system, and if the password hashes are stored there, it may allow a (malicious) user to try to perform a guessing attack to reverse the hashes to obtain passwords of other users.

The correct answer is 'False'.

### Question **2**

Correct

Mark 1.00 out of 1.00

Flag question

#### Question text

A SUID binary program in Linux, when run, may assume the effective uid of the owner user of the program.

Question 2

Select one:

True

False

#### Feedback

The correct answer is 'True'.

### Question **3**

Correct

Mark 1.00 out of 1.00

Flag question

#### Question text

In Linux, a user can create a symbolic link to a file even if the user does not have read access to the file.

Question 3

Select one:

True

False

#### Feedback

The correct answer is 'True'.

### Question **4**

Correct

Mark 1.00 out of 1.00

Flag question

#### Question text

In Unix/Linux systems, only the root user can change the owner user of a file to a different user.

Question 4

Select one:

True

False

#### Feedback

True. This is because certain access control features, such as the SUID/SGID bit, may allow a program to assume the effective UID or GID of the owner of the program when it is executed. If the non-root owner of a program can change the ownership of the program without any restriction, they can change the owner to root, and if the SUID bit is preserved after the change of ownership, that program, when executed, would assume the privilege of root.

The correct answer is 'True'.

### Question **5**

Correct

Mark 1.00 out of 1.00

Flag question

#### Question text

In a Unix/Linux system, the file /etc/passwd is readable only by the root user.

Question 5

Select one:

True

False

#### Feedback

The file /etc/passwd is readable by all users in the system.

The correct answer is 'False'.

### Question **6**

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

In a bash shell in Linux, what is the effect of setting the PATH environment variable as follows:

export PATH=/home/alice:$PATH

on the command 'ls' run in the same shell?

Question 6

Select one:

a.

The system will look for the command 'ls' in /home/alice first, unless it is an SUID program, in which case, the system will always use the command 'ls' in /bin/

b.

The PATH environment variable has no effect on which command gets executed.

c.

The system will look for the command 'ls' in /home/alice and prints an error message if the command is not found there

d.

The system will look for the command 'ls' in /home/alice last.

e.

The system will look for the command 'ls' in /home/alice first before searching other directories.

#### Feedback

Your answer is correct.

When a user executes a command in bash, without specifying the full path to the program (e.g., typing 'ls' instead of '/usr/bin/ls'), bash will check the existence of the 'ls' program in the directories listed in the PATH environment variable, from left to right. In this case, the path "/home/alice" will be checked first; if it is found there, then the 'ls' program in "/home/alice" will be executed. Otherwise, bash will continue searching the rest of the directories in PATH.

The correct answer is: The system will look for the command 'ls' in /home/alice first before searching other directories.

### Question **7**

Incorrect

Mark 0.00 out of 2.00

Flag question

#### Question text

Suppose a program produces files with default permission 642 (in octal notation) and suppose the umask set by a user is 044. What is the actual permission of the files produced by the program when run by the user? Give your answer in 3-digit octal notation.

Note: recall that when the permission bits are specified using a 3-digit octal, it is assumed implicitly that there are no special modes (i.e., all the bits in the special modes are 0).

Answer:

Question 7

#### Feedback

To calculate the actual permission of a file after the umask is applied, first invert the umask, and then perform a bit-wise AND operation with the default permission.

Umask: 044 --> 000 100 100

Inverted umask: 111 011 011

Default permission: 642 --> 110 100 010

Actual permission: (Inverted umask) AND (default permission) = (111 011 011) AND (110 100 010) = 110 000 010 --> 602 (in octal).

The correct answer is: 602

### Question **8**

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

Suppose Alice is a user in a Linux system. She creates a SUID binary program, `foo', that displays the content of a text file, `bar', in her home directory. Assume that the owner group of 'bar' is the group 'tutors', and that the file bar has the following permission (in textual notation): -rw------- (read/write access only for Alice and no one else). Assume also that Alice's home directory is readable and executable by everyone else, i.e., its permission bits (in textual notation) are: drwxr-xr-x.

She requires the program `foo' to be readable and executable by every user in the system, but is writeable only by herself. Furthermore, she wants the program `foo' to display the content of `bar', regardless of which user executes the program. What permissions should she give to the program `foo' to fulfil these requirements? Provide your answer in a 4-digit octal notation.

Answer:

Question 8

#### Feedback

Since the file "bar" is only readable/writeable by Alice, other users can't access it directly. The program "foo", if run by other users, will need to change its effective UID to that of Alice, in order for the program to be able to access "bar". This suggests that the SUID bit of "foo" needs to be set. The program "foo" also needs to be readable and executable by every user (this includes Alice, anyone in Alice's group, and everyone else), but writeable only by Alice. The following permission bits should fulfil this requirement:

Special modes: 100 (set the SUID bit)

Owner (Alice): 111 (read,write,exec)

Group: 101 (read, exec)

Other: 101 (read, exec)

So the complete permission bits are 100 111 101 101, which in octal notation is 4755.

The correct answer is: 4755

### Question **9**

Incorrect

Mark 0.00 out of 3.00

Flag question

#### Question text

Consider the following output of ls -l command in a Linux system:

alice@comp2700-lab:~$ ls -l  
total 44  
drwxr-xr-x 2 alice alice 4096 Sep 6 2015 Desktop  
drwxr-xr-x 2 alice alice 4096 Sep 6 2015 Documents  
drwxr-xr-x 2 alice alice 4096 Oct 9 20:37 Downloads  
-rw-r--r-- 1 alice alice 8445 Sep 6 2015 examples.desktop  
drwxr-xr-x 2 alice alice 4096 Sep 6 2015 Music  
drwxr-xr-x 2 alice alice 4096 Sep 6 2015 Pictures  
drwxr-xr-x 2 alice alice 4096 Sep 6 2015 Public  
drwxr-xr-x 2 alice alice 4096 Sep 6 2015 Templates  
drwxr-xr-x 2 alice alice 4096 Sep 6 2015 Videos  
alice@ubuntu32:~$ ls -l Downloads/  
total 4  
-rw------- 1 root root 6 Oct 9 20:36 rootfile  
alice@ubuntu32:~$

The user `alice' here is a non-root user. Which one of the following statements is true?

Question 9

Select one:

alice can read the content of `rootfile'

alice can delete 'rootfile'

alice cannot delete 'rootfile'

alice can modify the content of 'rootfile'

#### Feedback

Your answer is incorrect.

The operation of deleting a file is an operation on the directory, so to be able to delete a file, one needs write access to the directory the file is located. The file can be deleted even if the user does not have read/write access to the file.

From the output of "ls", we see that

drwxr-xr-x 2 alice alice 4096 Oct 9 20:37 Downloads

so the directory Downloads is owned by alice, and alice has "rwx" (read, write, execute) permissions, which means that alice can delete any files in that directory, regardless of who owns the files.

The correct answer is: alice can delete 'rootfile'

### Question **10**

Correct

Mark 3.00 out of 3.00

Flag question

#### Question text

Consider the following output of ls -l command in a Linux system, run by a user 'alice' in her home directory:

alice@comp2700-lab:~$ ls -l  
total 44  
drwxr-xr-x 2 alice alice 4096 Sep 6 2015 Desktop  
drwxr-xr-x 2 alice alice 4096 Sep 6 2015 Documents  
drwxr-xr-x 2 alice alice 4096 Oct 9 20:37 Downloads  
-rw-r--r-- 1 alice alice 8445 Sep 6 2015 examples.desktop  
drwxr-xr-x 2 alice alice 4096 Sep 6 2015 Music  
drwxr-xr-x 2 alice alice 4096 Sep 6 2015 Pictures  
drwxr-xr-x 2 alice alice 4096 Sep 6 2015 Public  
drwxr--r-- 2 root root 4096 Sep 6 2015 root\_private  
drwxr-xr-x 2 alice alice 4096 Sep 6 2015 Templates  
drwxr-xr-x 2 alice alice 4096 Sep 6 2015 Videos

Suppose that the directory root\_private contains a file called 'rootfile' with the following attributes (as output by a ls -l command):

-rw-r--r-- 1 root root 6 Oct 9 20:36 rootfile

The user `alice' here is a non-root user. Suppose alice runs the command 'cat root\_private/rootfile' in her home directory.

Which one of the following statements best describes the outcome of this command and the reason for that outcome?

Question 10

Select one:

The content of 'root\_private/rootfile' will be displayed because its permission bits indicate all users have read access to it.

A 'permission denied' error will be output, because alice does not have execute access to the directory 'root\_private', which is required to traverse to that directory in order to display the 'rootfile'.

A 'permission denied' error will be output, because alice does not have write access to the directory 'root\_private', which is required to traverse to that directory in order to display the 'rootfile'.

The content of 'root\_private/rootfile' will be displayed because its permission bits indicate all users have read access to it, and all users have read access to the directory 'root\_private', so alice can traverse to root\_private to display the file.

#### Feedback

Your answer is correct.

The directory root\_private is owned by root user and root group, and has the permission: drwxr--r--. Since alice is not a member of root group, her permission for the root\_private directory is determined by the 'other' part of the permission, i.e., r-- (read, no write, no exec). With no executable permission on root\_private, alice cannot change into that directory to perform any operation on it, and this includes displaying the content of root\_file, even if alice has read permission on the file.

The correct answer is: A 'permission denied' error will be output, because alice does not have execute access to the directory 'root\_private', which is required to traverse to that directory in order to display the 'rootfile'.

### Question **11**

Correct

Mark 3.00 out of 3.00

Flag question

#### Question text

Consider the following shell script, named `backdoor.sh':

===========

#!/bin/bash

/bin/cat /etc/shadow

===========

Suppose this shell is owned by user root, and has its permission set to 4755. Suppose this script is put in a directory where every user in the system has read and execute access. Suppose this script is run by a non-root user, bob. Which one of the following statements best describes the outcome of bob's attempt to run the shellscript?

Question 11

Answer

a.

A permission denied error occurs since the permission 4755 means the owner (root) has only read access to the shell script, not execute access right.

b.

A permission denied error occurs, since the SUID bit is ignored for shell scripts and the bob has no read access to /etc/shadow.

c.

The content of /etc/shadow is displayed, since the shell script executes under the effective UID of root, which has read access to /etc/shadow.

d.

The content of /etc/shadow is displayed since by default /etc/shadow is readable by everyone in the system.

#### Feedback

Your answer is correct.

The correct answer is:

A permission denied error occurs, since the SUID bit is ignored for shell scripts and the bob has no read access to /etc/shadow.

Consider a variant of the affine cipher where the alphabet consists of lower case letter 'a' to 'z', whitespace characters (newline, space and tab), and punctuations (question mark and exclamation mark). So we have a total of 31 symbols in the alphabet.

What is the size of the key space for this cipher?

Answer:

Question 1

#### Feedback

We map each character in the alphabet to 0,...,30 and encryption/decryption is done  
modulo 31.   
Recall that a key in this case is a pair (a,b) and encryption is done as follows:

 e_k(x) = a x + b  ~ mod ~ 31 

The pair k = (a,b) is a valid key if and only if a has a multiplicative inverse modulo 31, that is, gcd(a,31)=1.

Since 31 is a prime number, every number in {1,..,30} has an inverse modulo 31.   
Only the number 0 has no inverse mod 31.  
So we have 30 possibilites for a, and 31 possibilities for b.  
So total number of keys is 30x31 = 930.

The correct answer is: 930

### Question **2**

Correct

Mark 1.00 out of 1.00

Flag question

#### Question text

The multiplicative inverse of x modulo n exists if n is prime and n > x > 0.

Question 2

Select one:

True

False

#### Feedback

The correct answer is 'True'.

### Question **3**

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

Suppose we know that  x \times 9 \equiv 2 \mod 11 . Which one of the following correctly describes the value of  x ?

Question 3

Select one:

a.

 x \equiv \frac{9}{2} \mod 11 

b.

 x \equiv 2^{-1} \cdot 9 \mod 11 

c.

 x \equiv 2^{-1} \mod 11 

d.

 x \equiv 9^{-1} \cdot 2 \mod 11 

#### Feedback

Your answer is correct.

The correct answer is:  x \equiv 9^{-1} \cdot 2 \mod 11 

### Question **4**

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

The following cipher text was encrypted using the Caeser cipher.

ghezbvy unf rathysrq gur tnynpgvp erchoyvp  
gur gnkngvba bs genqr ebhgrf gb bhgylvat fgne  
flfgrzf vf va qvfchgr  
ubcvat gb erfbyir gur znggre jvgu n oybpxnqr bs qrnqyl  
onggyrfuvcf gur terrql genqr srqrengvba unf fgbccrq nyy  
fuvccvat gb gur fznyy cynarg bs anobb  
juvyr gur pbaterff bs gur erchoyvp raqyrffyl qrongrf  
guvf nynezvat punva bs riragf gur fhcerzr punapryybe unf  
frpergyl qvfcngpurq gjb wrqv xavtugf gur thneqvnaf bs  
crnpr naq whfgvpr va gur tnynkl gb frggyr gur pbasyvpg

The plaintext that corresponds to this cipher text was written in English. Decrypt this cipher text. What is the last word in the plain text you recovered?

Hint: you may want to use JCrypTool to help you with this question. Use 'Algorithms -> Classic -> Caesar'.

Answer:

Question 4

#### Feedback

The correct answer is: conflict

### Question **5**

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

Shift cipher or Caesar cipher can be made more secure if it is applied multiple times. For example, if the key space for the original cipher is 26, then applying encryption twice, with two different keys, increases the key space to 26 \* 26.

Question 5

Select one:

True

False

#### Feedback

Applying the shift cipher twice does not make it more secure; in this case the key space is still 26.

For example, if the first key is k1 and the second key is k2, then applying the encryption twice to a cipher text x is equivalent to

 \begin{align*}
e_{k1}(e_{k2}(x)) & = (x+k2) + k1 \mod 26 \\
  &  = x + (k1+k2) \mod 26 \\
  & = x + (k1+k2 \mod 26) \mod 26.
\end{align*}
 

So applying the cipher twice with two different keys is the same as applying it once with the key (k1+k2) mod 26. The key space is exactly the same: 26.

The correct answer is 'False'.

Modern block ciphers are structured in rounds of transformations that achieve the confusion and the diffusion operations. Which of the following transformations in AES corresponds to the confusion operation?

Question 1

Select one:

Inverse MixColumn

Key Schedule

ShiftRows

Byte Substitution

MixColumn

#### Feedback

Your answer is correct.

The correct answer is: Byte Substitution

### Question **2**

Correct

Mark 1.00 out of 1.00

Flag question

#### Question text

The multiplicative inverse of  x^6 + x^2 + 1  in  GF(2^8)  modulo  P(x) = x^8 + x^4 + x^3 + x + 1  is

Question 2

Select one:

 x^3 + x + 1 

 x^5 + x^4 + 1 

 x^5 + x^3 

 x^3 + 1 

 x^7 + x^6 + 1 

#### Feedback

Your answer is correct.

The correct answer is:  x^5 + x^4 + 1 

### Question **3**

Correct

Mark 1.00 out of 1.00

Flag question

#### Question text

What is the bit string representation of the polynomial  x^3 + 2x + 1   in GF(28)? Give your answer in the binary notation.

Answer:

Question 3

#### Feedback

The correct answer is: 00001001

### Question **4**

Correct

Mark 1.00 out of 1.00

Flag question

#### Question text

Which of the following is *not* true of the one-time pad cipher?

Question 4

Select one:

The encryption key must be as long as the message to be encrypted.

One-time pad can be implemented using AES in OFB mode.

One-time pad can be proved to be unconditionally secure.

Every encryption key can only be used once.

Encryption is done simply by applying the XOR operator to the key stream and the message.

#### Feedback

Your answer is correct.

The key used in one-time pad must be truly random; that is one of the main requirements of one-time pad. Using AES in OFB mode does not produce a truly random key stream; it produces a key stream from an initial seed of fixed length, so the key stream cannot be truly random. AES in OFB mode produces only pseudorandom key streams.

The correct answer is: One-time pad can be implemented using AES in OFB mode.

### Question **5**

Correct

Mark 1.00 out of 1.00

Flag question

#### Question text

If  A(x)= x^7+x^5+x^4+x^3+x+1   and  B(x)= x^6+x^4+x+1 . What is A(x)+B(x) in GF(28)? Give your answer in the binary notation.

Answer:

Question 5

#### Feedback

 A(x) + B(x) = x^7 + x^6 + x^5 + 2x^4 + x^3 + 2x + 2 \equiv x^7 + x^6 + x^5 + x^3  .

In binary representation: 11101000.

The correct answer is: 11101000

### Question **6**

Correct

Mark 1.00 out of 1.00

Flag question

#### Question text

There are no finite fields of order 12.

Question 6

Select one:

True

False

#### Feedback

The correct answer is 'True'.

### Question **7**

Incorrect

Mark 0.00 out of 1.00

Flag question

#### Question text

The AES block cipher, with the key size of 128 bits, combines 10 rounds of confusion-diffusion operations. At the minimum, how many rounds are needed so to ensure a good diffusion property, i.e., if one bit is flipped in the plaintext input, then around half of the bits in the output ciphertext will be flipped?

Question 7

Select one:

a.

9

b.

8

c.

2

d.

1

#### Feedback

Your answer is incorrect.

The correct answer is: 2

### Question **8**

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

If  A(x)= x^5+x+1  and  B(x)= x^4+x^2+1 . What is  A(x)\times B(x)  in GF(28) with modulus  P(x) = x^8+x^4+x^3+x+1 ? Give your answer in the binary notation.

Answer:

Question 8

#### Feedback

We first find the remainder of x^8 mod P(x) in GF(2^8):

 x^8 = P(x) - (x^4 + x^3 +1) \equiv x^4 + x^3 + x + 1 \mod P(x)
 

Then we substitute  x^4 + x^3 + x + 1  for  x^8  in A(x)B(x):

 \begin{align*}
A(x) \times B(x) & = (x^5 + x + 1) (x^4 + x^2 + 1) \\
 & \equiv x^9 + x^7 + x^5 + x^5 + x^3 + x + x^4 + x^2 + 1 \\
 & \equiv x^9 + x^7 + x^4 + x^3 + x^2 + x + 1 \\
 & \equiv x \cdot x^8 + x^7 + x^4 + x^3 + x^2 + x + 1 \\
 & \equiv x(x^4 + x^3 + x + 1) + x^7 + x^4 + x^3 + x^2 + x + 1 \\
 & \equiv x^5 + x^4 + x^2 + x + x^7 + x^4 + x^3 + x^2 + x + 1 \\
 & \equiv x^7 + x^5 + x^3 + 1  \mod P(x)\\
\end{align*}

 

In the binary notation this is 10101001.

The correct answer is: 10101001

### Question **9**

Correct

Mark 1.00 out of 1.00

Flag question

#### Question text

Consider a stream cipher generated using a linear congruential generator used in Exercise 5 in Lab 8. That stream cipher is used to encrypt a text file. The encrypted file is attached here ([quiz.enc](https://wattlecourses.anu.edu.au/pluginfile.php/3749336/question/questiontext/4057142/9/25215275/quiz.enc?time=1633057257203)). We know that the first word in the original unencrypted file is 'COMP2700' (without the quotes). Use this information to decrypt the file quiz.enc, and you will find the (numerical) answer to this question. Provide that answer in the provided answer box below.

Answer:

Question 9

#### Feedback

The correct answer is: 462

Which of the following AES encryption mode(s) is/are possible to be parallelised in terms of implementation?

Question 1

Select one or more:

CFB

CTR

ECB

CBC

OFB

#### Feedback

Your answer is incorrect.

The correct answers are: ECB, CTR

### Question **2**

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

If we are using AES in CTR mode to encrypt a file of size 232 bytes, how many bits we need to allocate to encode the counter, at a minimum, to ensure no counter is repeated?

Answer:

Question 2

#### Feedback

We know that the key stream generated from the CTR mode is done per block (16 bytes). So each counter value can generate one block (= 16 bytes) of key streams. To encrypt 2^32 bytes, we need 2^32/16 = 2^28 blocks of key streams to avoid a counter value being re-used.

The correct answer is: 28

### Question **3**

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

In OFB mode, reusing the same key and IV to encrypt different messages can potentially compromise secrecy of the messages if the plaintext of one of the messages is known to the attacker.

Question 3

Select one:

True

False

#### Feedback

The correct answer is 'True'.

### Question **4**

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

In CBC encryption mode, if the IV is not reused to encrypt different messages, then its value does not need to be kept secret in order to protect the secrecy of the encrypted message.

Question 4

Select one:

True

False

#### Feedback

The correct answer is 'True'.

### Question **5**

Correct

Mark 1.00 out of 1.00

Flag question

#### Question text

Which of the following statements are true of the ECB encryption mode? Select all applicable answers.

Question 5

Select one or more:

a.

When using ECB to encrypt a message of length greater than one block, each block can be encrypted independently of the other blocks.

b.

Choosing a random IV is important to ensure the security of ECB

c.

ECB ensures the integrity of the ciphertext, that is, it is not possible to modify the ciphertext that would decrypt to a meaningful message without knowing the encryption key.

d.

ECB may reveal a pattern in the underlying plaintext if the size of the plaintext is larger than the block size of the cipher.

e.

ECB mode does not require an IV.

#### Feedback

Your answer is correct.

The correct answers are: ECB may reveal a pattern in the underlying plaintext if the size of the plaintext is larger than the block size of the cipher., When using ECB to encrypt a message of length greater than one block, each block can be encrypted independently of the other blocks., ECB mode does not require an IV.

### Question **6**

Correct

Mark 1.00 out of 1.00

Flag question

#### Question text

Consider the following 12-byte input (represented as a HEX string, with spaces added for clarity):

01 aa b2 c2 01 cd e8 d9 ff 23 87 00

If this were to be passed on to AES for encryption, it needs to be padded. Suppose we use the PKCS#7 padding scheme. What would be the padded message?

Question 6

Answer

a.

01 aa b2 c2 01 cd e8 d9 ff 23 87 00 04 04 04 04

b.

01 aa b2 c2 01 cd e8 d9 ff 23 87 00 04

c.

01 aa b2 c2 01 cd e8 d9 ff 23 87 00 00 00 00 00

d.

01 aa b2 c2 01 cd e8 d9 ff 23 87 00 06 06 06 06

#### Feedback

Your answer is correct.

The correct answer is:

01 aa b2 c2 01 cd e8 d9 ff 23 87 00 04 04 04 04

Suppose H is a hash function with 512-bit output. If we are going to find a collision attack for H by brute force, how many hash values need to be randomly generated, on average, in order to have a 50% chance of finding a collision?

Question 1

Select one:

a.

 1.177 \times 2^{256}  

b.

 1.177 \times 10^{128} 

c.

 1.177 \times 2^{512}  

d.

256

e.

128

#### Feedback

Your answer is correct.

The correct answer is:  1.177 \times 2^{256}  

### Question **2**

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

Consider the following construction of a MAC: the MAC of a message m under the key k is defined as follows:

MAC(m,k) = H(k || c || m)

where H is a hash function constructed using Merkle-Damgard construction, c is a block of 0's of length 128 bits, and || refers to the concatenation operator on bit strings.

This MAC construction is vulnerable to a forgery attack. That is, if the attacker learns the value of m and MAC(m,k), then the attacker will be able to construct a message m', distinct from m, and its MAC, without knowing the key k.

Question 2

Select one:

True

False

#### Feedback

True.

This MAC construction is essentially based on the secret prefix construction. Since H is based on Merkle-Damgard construction, the scheme is vulnerable to the message extension attack.

The correct answer is 'True'.

### Question **3**

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

Any collision attack on a hash function H can be turned into a second-preimage attack on the same hash function H.

Question 3

Select one:

True

False

#### Feedback

The correct answer is 'False'.

### Question **4**

Correct

Mark 3.00 out of 3.00

Flag question

#### Question text

Consider the hash function ecbhash used in Exercise 3 of Lab 10. Suppose you have a message m obtained by concatenating 2 16-byte messages x and y. That is,

m = x || y

where || denotes the concatenation operator on bit strings.

Assume that x and y are distinct messages.

Which one of the following constructions will definitely produce a second pre-image of m?

Question 4

Select one:

a.

x || x || y

b.

x || x

c.

x || x || y || x

d.

y || y

e.

y || x || y

#### Feedback

Your answer is correct.

The correct answer is: x || x || y || x

### Question **5**

Incorrect

Mark 0.00 out of 3.00

Flag question

#### Question text

Consider the function cbcmac from Exercise 6 in Lab 10. Suppose you are given the following input string (written in Python notation):

m = b'CBCMAC is broken'

(which is exactly 16 bytes), and its MAC (represented as a HEX string), created using an unknown key:

fa72eea8123d57107ebfe1918bf7241c

Construct a two-block input that has the same MAC as m (under the same MAC key) using the CBC-MAC attack discussed in this lab. Write your answer as a HEX string.

Note that the IV value of cbcmac is hard-coded in cbcmac.py, i.e., it is fixed to the following value:

b'fedcba9876543210'

The attacker is assumed to know this value (since the algorithm is supposed to be public).

NOTE: *you need to provide your answer as a HEX string. If you use python scripts to create the input bytes (as shown in the lab 10 solution), make sure you convert the bytes to hex string, e.g., using the hex() function. For example, if the input you constructed is the bytes (in python notation) b'abc\x01', then its HEX string would be 61626301.*

Answer:

Question 5

#### Feedback

The correct answer is: 4342434d41432069732062726f6b656edf55c986311f4e413aa9b6d7d7ae7042

What is the value of  \Phi(70)  ?

Answer:

Question 1

#### Feedback

The correct answer is: 24

### Question **2**

Correct

Mark 1.00 out of 1.00

Flag question

#### Question text

Which one of the following is a primitive element of the cyclic group  Z_{17}^*  ?

Question 2

Select one:

a.

4

b.

2

c.

1

d.

5

#### Feedback

Your answer is correct.

The correct answer is: 5

### Question **3**

Correct

Mark 1.00 out of 1.00

Flag question

#### Question text

Consider the following parameters for RSA: p=11, q=23, e=17. Compute the private key given these parameters.

Hint: You can use python to help you calculate multiplicative modular inverse. See Lab 8 guide for some examples.

Answer:

Question 3

#### Feedback

The correct answer is: 13

### Question **4**

Correct

Mark 1.00 out of 1.00

Flag question

#### Question text

In RSA, two randomly generated prime numbers p and q are used to generate the modulus  n = p \times q   and  \Phi(n ) .

The value of  \Phi(n )  can be made public without compromising the security of RSA.

Question 4

Select one:

True

False

#### Feedback

The correct answer is 'False'.

### Question **5**

Correct

Mark 1.00 out of 1.00

Flag question

#### Question text

In practice, when choosing the public exponent e for RSA, often a small number is chosen as the value for e. What is the main reason for this choice?

Question 5

Select one:

a.

To make sure that decryption with the private key can be performed efficiently.

b.

To guarantee that the decryption key will always be a prime number.

c.

To make it harder to compute the prime factors of the modulus used in RSA.

d.

To ensure that encryption with the public key can be performed efficiently.

#### Feedback

Your answer is correct.

The correct answer is: To ensure that encryption with the public key can be performed efficiently.