NIA 2023P PAC3 solution

Redes y aplicaciones Internet (Universitat Oberta de Catalunya)

Bachelor's Degree in Techniques for Software Development

Network and Internet Applications
PAC 3 - Third Continuous Evaluation Test

- The solution should be delivered preferably in a pdf file, using the corresponding template, in the continuous evaluation registry.
- Limit date for delivery is June 4th 2023.

Answers

1. SIP and RTSP protocols are application level protocols that share some characteristics. Indicate whether the following questions are true or false. If they are false, describe why they are false.

a) The two protocols use the same request/response message structure.
b) Both SIP and RTSP could be changed by another application level protocol, which is HTTP.
c) The 200 OK code is a valid response code in both protocols.
d) The RTSP protocol requires a proxy in order to establish communication between a client and a server.
e) The RTSP protocol is currently one of the most widely used protocols to control video streams on YouTube or Netflix.

a) True.
b) False. The three protocols have different purposes and commands, so it is not possible to interchange them. However, they share some characteristics, such as message structure and response codes.
c) True.
d) False. In the SIP architecture it may be necessary to use a proxy and also a registrar in order to establish communications.
e) False. Both Youtube and Netflix use MPEG DASH to control *streams*.

2. In order to have a functional VoIP service it is necessary that end-to-end delay does not exceed certain values. Please answer the following questions in a reasoned manner:

a) What delay values make a VoIP service unviable?
b) Which network elements are involved in end-to-end delay? Indicate what type of delay each of them introduces.
c) Go to the website https://gaia.cs.umass.edu/kurose_ross/interactive/end-end-delay.php and answer at least two of the questions. Paste the screenshots corresponding to the answers and justify the results.

a)
More than 400 ms makes it unfeasible. Below 150 ms is imperceptible to the human ear. Between 150 ms and 400 ms is acceptable.

b)
Routers: transmission delays, processing and queuing.
Links: propagation delays.
Final systems: processing delays at the transmitter and receiver.

c)
Free answer depending on the exercises chosen.

3. Chapter *9.5.4 Per-Connection Quality-of-Service (QoS) Guarantees: Resource Reservation and Call Admission* in the course book mentions the *Resource Reservation Protocol* (RSVP) for resource reservation.

a) Find information about RSVP and its use in today's networks.
b) Check if this protocol appears in the screenshots of Practical exercise 1.
c) If so, show the values it carries. If not, find out which are the most common values.

Free answer.

4. Find information on how to find out if your home or work router has Quality of Service (QoS) mechanisms activated and briefly describe them. Indicate all the sources of information you have consulted.

Free answer that depends on the router model you have.

5. Find information about which network and application protocols are used in online multiplayer games. Explain how the use of one protocol or another affects the players' experience and what kind of information is transmitted with each protocol, depending on the criticality of the information sent during the development of the game. Copy all the links from where you have extracted information.

Free answer depending on the architecture of the game and the protocols found.

6. Briefly explain the following attacks: “Ciphertext-only attack”, “Known-plaintext attack” and “Chosen-plaintext attack”. Why do you think that in the last example the sentence “The quick brown fox jumps over the lazy dog” (or “*Es extraño mojar queso en la cerveza o probar whisky de garrafa*” in the Spanish version) is used?

- Ciphertext-only attack. In some cases, the intruder may have access only to the intercepted ciphertext, with no certain information about the contents of the plaintext message. We have seen how statistical analysis can help in a ciphertext-only attack on an encryption scheme.
- Known-plaintext attack. We saw that if Trudy somehow knew for sure that “bob” and “alice” appeared in the ciphertext message, then she could have determined the (plaintext, ciphertext) pairings for the letters a, l, i, c, e, b, and o. Trudy might also have been fortunate enough to have recorded all of the ciphertext transmissions and then found Bob's own decrypted version of one of the transmissions scribbled on a piece of paper. When an intruder knows some of the (plaintext, ciphertext) pairings, we refer to this as a known-plaintext attack on the encryption scheme.
- Chosen-plaintext attack. In a chosen-plaintext attack, the intruder is able to choose the plaintext message and obtain its corresponding ciphertext form. For the simple encryption algorithms we've seen so far, if Trudy could get Alice to send the message, “The quick brown fox jumps over the lazy dog,” she could completely break the encryption scheme. Anyway, for more sophisticated encryption techniques, a chosen-plaintext attack does not necessarily mean that the encryption technique can be broken.

The sentence “The quick brown fox jumps over the lazy dog” (or “*Es extraño mojar queso en la cerveza o probar whisky de garrafa*”) is used because it is a pangram: it includes all the letters of the English alphabet (or Spanish in the second case).

7. Compare the similarities between the mathematical operations used in RSA and those used in the Diffie-Helmann mechanism.

RSA encrypts the message by raising it to the key and calculating a modulo:
X = (M^k) mod n

The Diffie-Helmann mechanism is also based on the exponentiation of a number followed by the calculation of the modulo.
First, both Alice and Bob apply it to a generator number (g) and its random number (a or b, respectively):
Alice: A = (g^a) mod p
Bob: B = (g^b) mod p

And then, to obtain the symmetric key (K), they apply it again with the number received from the other user (B and A, respectively) and their random number:
Alice: K = (B^a) mod p
Bob: K = (A^b) mod p

8. Go to the following website:

https://www.devglan.com/online-tools/rsa-encryption-decryption

Generate a 512-bit asymmetric key pair (the drop-down reads 515).
To the RSA Encryption part:

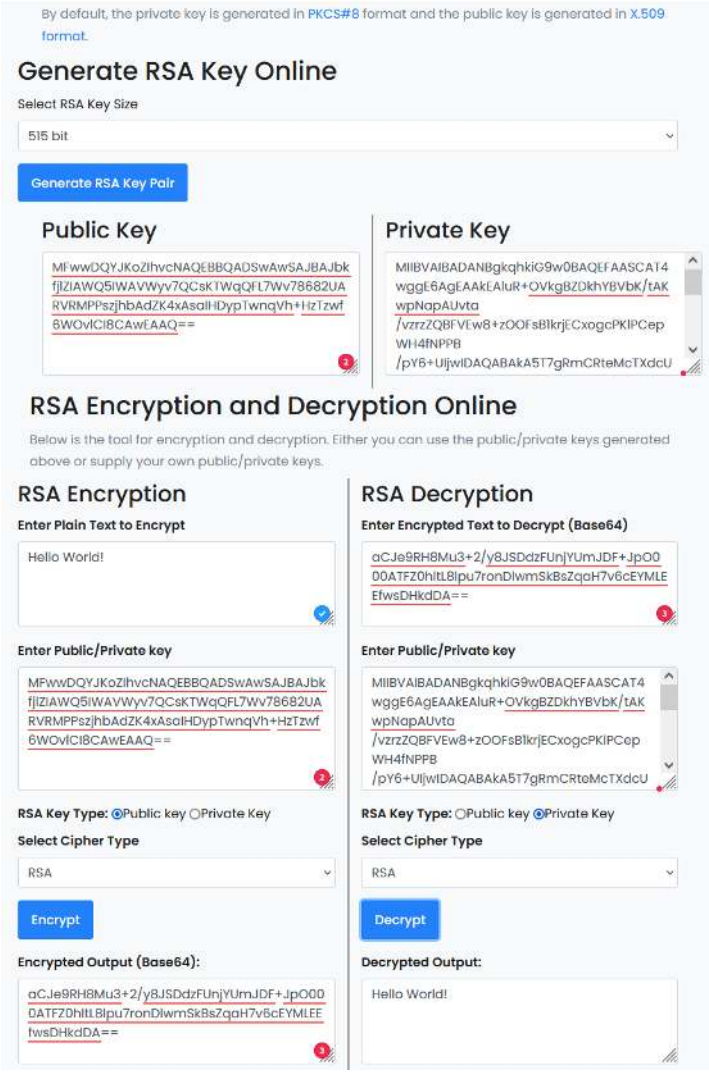
- Under “Enter Plain Text to Encrypt”, enter a very short text including your first (or last) name.
- Set one of the two keys (public or private) in “Enter Public/Private key” and select the key type.
- Select “RSA” in “Select Cipher Type”.
- Click “Encrypt”.

In the RSA Decryption part:

- Copy the encrypted text from the previous step into “Enter Encrypted Text to Decrypt (Base64)”.
- Enter the complementary key you have set in the encryption section under “Enter Public/Private key” and select the type of key.
- Select “RSA” to “Select Cipher Type”.
- Click “Decrypt”.
- Check that the decrypted text is the same as the text you encrypted.

a) Put a screenshot where you can see all the fields filled in.
b) Say whether you have chosen to use the public or private key first and say what security you will get in this case.
c) Why does the output actually have 512 bits (88 characters in base64, with 2 '=' at the end) when the input has only 12?
d) Now, change the first character of “Enter Encrypted Text to Decrypt (Base64)” and click “Decrypt”. What message do you get? Justify it and say what security service it provides.
e) Then click “Encrypt” again, why does it give a different string? Even though it is a different string, can you decrypt it with the same key? Take a screenshot and explain why this is the case.

a)



b)
Public key: confidentiality and integrity
Private key: integrity and authentication

c)
Because RSA is based on block ciphers, in this case 512 bit, and the output is always multiple of the number of bits in a block.

d)
“Decryption error”. The message has changed, and cannot be decrypted -> Integrity

e)
Yes, it can be decrypted.
A secure RSA encryption is implemented with an appropriate padding scheme, which includes some randomness. It encrypts message padded with '0's and a string of random bit.

9. We have the following secure PGP message:

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256
```

```
Hello World!
-----BEGIN PGP SIGNATURE-----
Version: OpenPGP.js v1.0.1
Comment: http://openpgpjs.org

wpwEAQEIABAFAmQ5TroJEJr48KCYYDt0AADT6gP9EHWmxGgBGrkbFqKNbgjL
yiozSXioCxTMbC9lAY/FiiERWL8RBJF1WsEHh0pRlPMloRi0hgwXx8Tu15h0
MxRaMHy6h2qU+BI8+5NrtbalFcJLqAF5TesjjRmikfYeOJP3t255q2F2H/D3
agzc1bMA4QHPJBuENIwdpgPkFwbdpfs=
=XFNP
-----END PGP SIGNATURE-----
```

a) Why can we see the text, if we said it was a secure message? How secure is it?
b) Why do you specify that you use a *Hash* function (SHA256) (Why do you need a Hash function?).
c) Explain the operation of the security mechanism used in this message, both in transmission and reception.

a) Because it is only signed. It has origin and integrity authentication.

b) Because the signature uses a hash function.

c) Encrypt with the sender's secret key the *hash* of the message and attach it to the message.
On reception, the signature is decrypted with the sender's public key, obtaining the hash of the original message, which is compared with the hash of the received message (*hash* calculated by the receiver).

10. The following sentences are false, as they include one term associated with security, but the definition of another.
Propose the 2 possible corrections for each of the sentences (in the solution, underline or mark the parts that you have changed from the original sentence to correct them).

a) In block cipher, data is encrypted continuously, without being split into blocks.
b) The length of an encrypted message is always fixed and small, and independent of the length of the original message.
c) Asymmetric encryption of a message with Bob's public key, K+B (or KBp), provides source authentication and integrity.
d) The best way to obtain confidentiality of a message is to use digital signature.
e) A digital signature serves to ensure that data, including a public asymmetric key and user data, correspond to a specific user.

a) In block cipher, data is split and encrypted in chunks (blocks).
In stream cipher, data is encrypted continuously, without being split into blocks.

b) The length of the hash of a message is always fixed and small, and independent of the length of the original message.
The length of an encrypted message is always "equal" [approximately equal, perhaps a few octets longer] to the length of the original message.

c) Asymmetric encryption of a message with Bob's secret key, K-B (or KBs), provides source authentication and integrity.
Asymmetric encryption of a message with Bob's public key, K+B (or KBp), provides confidentiality and integrity.

d) The best way to obtain confidentiality of a message is to use symmetric encryption.
The best way to obtain origin authentication and integrity of a message is to use digital signature.

e) A digital signature serves to authenticate the origin and to verify that a message has not been modified.
A digital certificate serves to ensure that data, including a public asymmetric key and user data, correspond to a specific user.