Remember: wrong answers come along with a penalty (negative points). No answer = no penalty (0 points).

Quesito 1
In a digital signature, the authentication tag is produced using
- **a)** The CA certificate
- **b)** The signer's certificate
- **c)** The signer's private key
- **d)** The signer's public key

Quesito 2
What is the advantage of a digital signature with respect to symmetric authentication using HMAC?
- **a)** The digital signature further guarantees the non-repudiation property
- **b)** The digital signature further guarantees the encryption of the signed message
- **c)** The digital signature further guarantees the protection of the signer's identity
- **d)** The digital signature further guarantees the protection against a MITM attacker

Quesito 3
Why Encrypt-and-MAC is a poor approach?
- **a)** Because the MAC tag is not encrypted
- **b)** Because the MAC tag is deterministic
- **c)** Because the MAC tag is performed with the same key as encryption
- **d)** Because the MAC tag is performed without any key

Quesito 4
TLS prevents replay attacks by:
- **a)** Including a sequence number in each TLS record header
- **b)** Concatenating TLS fragments using as Initialization Vector the previous finished message
- **c)** Using sequence numbers in the HMAC computation
- **d)** Including a random nonce in each TLS fragment

Quesito 5
Given N data units (chunks), the number of siblings in a (balanced) Merkle tree is
- **a)** Log10(N)
- **b)** N
- **c)** N/2
- **d)** Log2(N)

Quesito 6
Why RSA is broken if the factorization N=p x q is revealed? (assume that e is the public key and d is the private key)
- **a)** Because it becomes possible to compute d = -e mod p x q
- **b)** Because it becomes possible to compute d = 1/e mod p x q
- **c)** Because it becomes possible to compute d = 1/e mod (p-1)(q-1)
- **d)** Because it becomes possible to compute d = -e mod (p-1)(q-1)

Quesito 7
In PKI, CRL stays for
- **a)** Certificate Recording Ledger
- **b)** Certificate Repository Library
- **c)** Certificate Revocation Label
- **d)** Certificate Revocation List

Quesito 8
When using IPsec ESP, the part of an IP packet left unencrypted is:
- **a)** Nothing – all the packet including the IP header is encrypted
- **b)** Only the IP header; all the IP payload is encrypted
- **c)** The IP header and the IPsec SPI
- **d)** The IP header, the IPsec SPI, and the IPsec Sequence number

Quesito 9
The TLS renegotiation attack permits to…
- **a)** Inject arbitrarily chosen plaintext in any arbitrary point during the victim's TLS session
- **b)** Detect whether the victim's plaintext includes a given pattern (e.g. strings such as 'twitter-id=flavia')
- **c)** Inject arbitrarily chosen plaintext before the start of the victim's TLS session
- **d)** Truncate a TLS connection in a way that the receiver does not detect such truncation

Quesito 10
Three of the following four statements are wrong about a dynamic IPsec IKE configuration with PSK: which is the only one correct?
- **a)** Initiator and responder MUST SHARE a same certificate from the CA
- **b)** The responder is NOT required to know the Initiator's IP address;
- **c)** Initiator and responder MUST SHARE the CA private key
- **d)** Itinitiator and responder MUST both have a public IP address

Quesito 11
In TLS v1.3, when using PSK, Perfect Forward Secrecy may be guaranteed…:
- **a)** by exchanging two fixed (and signed by a CA) DH coefficients g^x and g^y and by deriving the session keys as $HKDF_{psk}(g^{xy})$
- **b)** by exchanging two ephemeral non-signed DH coefficients g^x and g^y and by deriving the session keys as $HKDF_{psk}(g^x , g^y)$
- **c)** by exchanging two fixed (and signed by a CA) DH coefficients g^x and g^y and by deriving the session keys as $HKDF_{psk}(g^x , g^y)$
- **d)** by exchanging two ephemeral non-signed DH coefficients g^x and g^y and by deriving the session keys as $HKDF_{psk}(g^{xy})$

Quesito 12
In IPsec IKE, a peer receives an IKE version N message with the V flag set to 1. This means that:
- **a)** the other peer is able to support only version V=1
- **b)** the other peer is able to support a version greater than N
- **c)** there is for sure a version downgrade attack in progress.
- **d)** the other peer is able to support at most version N

Quesito 13
The expand phase in key derivation permits to:
- **a)** compute the nonces to be exchanged during the TLS handshake
- **b)** derive multiple session keys from a single master key and the exchanged nonces
- **c)** expand a same TLS session across multiple TCP connections
- **d)** derive the master key from the pre master key and the exchanged nonces

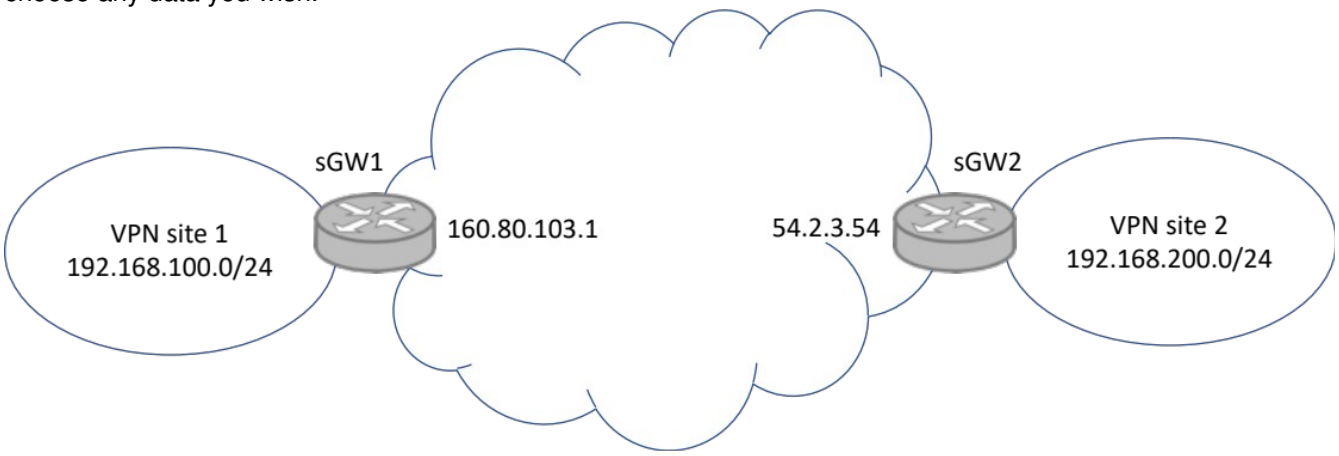
Quesito 14

The type of attack at the basis of the TLS BEAST attack is a…
- **a)** Chosen Key Attack
- **b)** Chosen KeyStream Attack
- **c)** Chosen Ciphertext Attack
- **d)** Chosen Plaintext Attack

Quesito 15
The TLS close-notify message addresses the following problem:
- **a)** An attacker may replay a previous TCP segment and circumvent TLS integrity
- **b)** An attacker may spoof a TCP RST and abort the underlying TCP connection before the end of the legitimate TLS session
- **c)** An attacker may spoof a TLS Client Hello and renegotiate the connection parameters before the end of the legitimate TLS session
- **d)** An attacker may spoof a TCP FIN and close the underlying TCP connection before the end of the legitimate TLS session

Quesito 16
The secret used in the HKDF is technically included in the HKDF construction as…
- **a)** Initial seed for the first HMAC block
- **b)** hashed message for each internal HMAC block
- **c)** Context string for all the HMAC blocks
- **d)** key of each internal HMAC block

Es. 1 (IPsec VPN). List the entries in the Security Association DB and the Security Policy DB on sGW1 assuming that we have successfully configured a VPN GW2GW between VPN Site 1 and 2 (see the topology in figure). Security association(s) are assumed to be in tunnel mode with ESP and both authentication and encryption enabled. If some data is missing (e.g. SPI, keys, algorithms, etc) you can choose any data you wish.



Es. 2 (TLS Padding Oracle Attack) – Assume a CBC-based block encryption scheme which uses block sizes of 4 bytes each. Assume that the attacker sees the following ciphertext (hex notation):

f1 aa 11 04 || 34 35 f1 20 || 11 01 9c 01 || ac c3 83 02 || 65 61 fb 08 || 91 11 5f 10

Assume now that the server is vulnerable to a Padding Oracle attack. The goal of the attacker is to check whether the plaintext corresponding to the sixteenth byte (the underlined byte, i.e. the byte whose ciphertext is 02) is the byte 0x0f hex = 00001111 binary. Which Chosen ciphertext message should the attacker send to the server/oracle, and why?