- In digital signature schemes, compromising the integrity of the signing key does not compromise the security of the algorithm
    - Answer: False

- If you are using the Tor browser with default configurations through the wireless network of Concordia, the IT staff cannot determine that you are using Tor
    - Answer: False. With the default configurations you will use a relay with an IP address that is publicly known, so all Concordia has to do is check if you're connecting to one of those relays. To be secret, you would have to configure Tor to use the secret bridge relays.

- In RSA cryptosystems, we can publish p and q to help the sender speedup the encryption operations using Chinese Remainder Theorem
    - False. If you publish P and Q then you break the integrity of the cryptosystem.

- The IP addresses of all the available Tor relays has to be kept secret
    - False. Tor bridges are relays whose IP addresses are kept secret so that people in countries that block known TOR IPs can still use it. But many relays have public IP addresses and can be used safely.

- When using Shamir Secret Sharing Scheme, we can set the Threshold to be greater than the number of shares (shadows)
    - False.
        - Shadows is the total number of shares created
        - Threshold is the number of shares required to find the key
        - You cannot require more shares than you created

- The One Time Pad system can be broken by a quantum computer
    - Answer: False. Without knowing the pad, a ciphertext can correspond to any message.

- In Crowds, the proxies (Jondos) know the final destination of the messages
    - Answer: True, though they don't know the source.

- Digital Signature Schemes can be used to achieve authentication, data integrity, and non-repudiation
    - Answer: True

- In RSA cryptosystems, the key setup operations are performed by the sender

    - False. It is formed by the receiver.

- Running a Tor exit node is more likely to put you into trouble with law enforcement agencies compared to running a Tor guard node
    - Answer: True. You're the one who will be sending all the sketchy packets to the destination.

- The security of a digital signature scheme is compromized if the underlying hash function is broken
    - Answer: True.

- The use of "redundant scanning" allows for faster spreading of computer worms
    - Answer: False. Reducing redundant scanning will speed up the spread of worms.

- The weak collision resistance property of a hash function h states that given an arbitrary x1, it is hard to find x2 (with x1 not equal to x2) such that h(x1) = h(x2)
    - True

- Computer viruses are standalone malware and they do not require a host program to propagate.
    - Answer: False. They require a host.

- The strong collision resistance property of a hash function h states that there exists no x1 and x2 (with x1 not equal to x2) such that h(x1) = h(x2)

- The use of SSL/TLS ensures the source and destination anonymity
    - Answer: False. They don't provide source or destination anonymity.

- When using TOR to connect to a hidden service, the IP address of the TOR hidden service will be known to your TOR browser
    - Answer: False

- Primality testing, i.e., deciding whether a given number n is prime or composite, is a hard problem
    - false

- Consider a toy RSA system with p=5, q=11 and e=7. The ciphertext corresponding to m=3 is equal to
    - **42** <<
    - 41

- Consider a toy RSA system with p=5, q=11 and e=7. The decryption exponent d is equal to :
    - **8**
    - 23

- Let E be a block cipher that encrypts a 32-bit message under a 64-bit key. To encrypt 64-bit message, the message M is split in two parts M1 and M2 and the key K in two parts K1 and K2. The ciphertext C s then computed as **EK1(M1) || EK2(M2)**, where **EK(M)** means encrypting M using E with a key K, and || denotes a concatenation operation. Assume we know that C is the encryption of the 64-bit message M. Then this system can be broken in
    - 2^65 steps
    - **2^33 steps**

- Message Authentication codes (MAC) can be used to achieve non-repudiation:
    - FALSE