# SVGS Computer Security, Cryptology Quiz

My motive in writing this quiz is simple, to get students to review the slides. This test is open book. The questions are in the same order that the slides are in.

1. Why did WEP fail?
2. What is wrong with this statement? “I used base64 encryption to hide my data.”
3. How is the modular inverse of a number usually calculated?
4. What is the modular inverse of 5 mod 13 ? You can use Python or a calculator
5. What is the most important thing to remember about an IV or nonce?
6. What is wrong with AES-ECB mode?
7. What advantage does symmetric key encryption have over asymmetric key encryption? What disadvantage?
8. What is non-repudiation?
9. Why isn’t RSA used for encrypting large data files?
10. With RSA encryption, if Alice sends a message to Bob, she encrypts the message with…
11. How do computers get the large prime numbers they use in encryption? How do they know they are really prime?
12. What is Φ(n)? If n is the product of primes 17 and 23, what is Φ(n)? You can use λ(n) if you prefer.
13. Why is a good PRNG important in cryptography?
14. What is the most popular Key exchange method for HTTPS? For SSH? (Diffie-Hellman slides may be helpful.)
15. Is Elliptic Curve Cryptography more closely related to Diffie-Hellman or to RSA cryptography?
16. What are the public portions of a key exchange using Elliptic Curve Cryptography?
17. What is the primary difference between a digital signature and a MAC (Message Authentication Code, not MAC address)?
18. What are the two properties a cryptographic hash is supposed to have?
19. A Digital Certificate is used to distribute a …
20. Why is it important to know where a public key really came from?
21. When a browser uses HTTPS, how does it know it is talking to the correct server and not an imposter?
22. A browser and a server agree on a cipher suite instead of just saying ‘TLS’. What are the different protocols in the suite used for?
23. In TLS the network traffic is encrypted, and the school’s/company’s IPS cannot inspect the data to see if it is malware. What information is available (at least in TLS v1.2 and below) that can give some clues to network security personnel?
24. What key exchange protocols may be used for ‘Perfect’ Forward Secrecy? What protocol may not be used?