IMPORTANT: The following is a set of sample questions for the exam to give you an idea however certain changes may be introduced in the actual exam regarding the question style/format/number and alike!

Instructions:
The exam has a duration of **2 hours**. There are 30 - 35[1] MC and MA (multiple answer) type of questions and 1-3[2] open-ended questions.

If you think that an MC question has multiple correct alternatives select the most specific one!

Provide concise answers to the open question/s (not available in the samples). A needlessly long and verbose answer results in a lowered grade.

In the questions[3]:

`'pow(x, y)'` `is used to indicate x raised to the power y;`
`'x mod y'` `is used to represent the remainder of the integer division of x by y`

Good Luck!

[1] actual number to be determined
[2] actual number to be determined
[3] This may also change

1. For the RUG 'defense in depth' is exemplified by

(a) spam filters installed by Google, SURF, and your own computer

(b) deep packet inspection of network traffic performed by system administrators

(c) deep packet inspection of network traffic performed by the outer RUG firewall computer

(d) routing all wireless network traffic through a single core router before connecting to the Internet

2. It takes time to recover from information security attacks. What type of attacks take the most time to resolve?

(a) Attacks performed by insiders

(b) Denial of service attacks

(c) Phishing attacks

(d) Virus attacks

3. The transposition ciphers covered by the lectures and Mark Stamp's book are characterized by the fact that characters

(a) of the plain text are replaced by other characters

(b) in rows of the plain text matrix reappear in rows of the encrypted text matrix

(c) in columns of the plain text matrix reappear in rows of the encrypted text matrix

(d) in the plain text matrix reappear in random locations of the encrypted text matrix.

4. With Feistel ciphers blocks are split in left and right halves. If only one encryption round is used, then

(a) the left half is not modified and becomes the left half in the next round, whereafter the key schedule is applied to the left half in the next round.

(b) the left half is not modified and becomes the right half in the next round

(c) the right half is not modified and becomes the right half in the next round, whereafter the key schedule is applied to the right half in the next round.

(d) the right half is not modified and becomes the left half in the next round

5. (Using Ci to indicate the i-th encrypted block, Pi to indicate the i-th plain text block) Information leakage can be a problem with the CBC block cipher mode.

(a) If Pi is equal to Pi+1 then the corresponding encrypted blocks are also identical

(b) If Ci is equal to Cj then Pi is equal to Pj

(c) If Ci is equal to Cj then Pi xor Pj is known

(d) If Ci is equal to Cj then Pi xor Pj equals Ci-1 xor Cj-1

6. A linear diophantine equation xe + yf = g uses e = 4, f = 8. Once the equation is solved for x and y then an alternative solution for x and y

(a) does not exist, as solutions of linear diophantine equations are unique

(b) can be 8 + x and -4 + y

(c) can be 4 * x and -4 * y

(d) can be 8 * x and -8 * y

7. When Alice and Bob use Ephemeral Diffie-Hellman

(a) They send their computed pow(g, x) mod p to their partner, and then destroy both their x and pow(g, x) mod p values.

(b) They compute their x that is used in pow(g, x) mod p, and send x, encrypted with their shared encryption key K to their partner.

(c) After obtaining their partner's pow(g, x) mod p they use their own y to compute pow(g, xy) mod p.

(d) They must make sure that their shared encryption key K is not compromised, or an attacker will be able to retrieve the session key

8. When computing pow(333, 29) mod 17

(a) you can compute pow(333 mod 17, 29) instead

(b) you can compute pow(333, 29 mod 17) instead

(c) start with the least significant bit of 29

(d) start with the most significant bit of 29

9. Which of the following hashing algorithms is considered cryptographically strong?

(a) The Cyclic Redundancy Check

(b) MD5

(c) Both a and b

(d) Neither a nor b.

10. To compute a HMAC value of a message M using key K and hash function h(A, B) where A represents a message and B represents a key, then the hash value should be computed as

(a) h(K, M)
(b) h(M, K)
(c) h(K, h(K, M))
(d) h(M, h(M, K))

11. Which of the following is *not* a 'role' in OAuth2?

(a) Relying Party
(b) Resource owner
(c) Client
(d) Authorisation Server

12. Using Kerberos, replay attacks are prevented by

(a) the ticket-granting server sending a 'lifetime' to the client
(b) the client sending a timestamp to the service provider
(c) the service provider sending a timestamp to the client
(d) using separate encryption keys for all communication between client, service provider, ticket-granting server and authentication server

13. Alice and Bob agree on using K, a shared encryption key. Also, they may use ephemeral Diffie-Hellman. For each new session they agree to use a separate encryption key Y. When Alice constructs Y, which protocol should not be used to inform Bob about Y? **Note**: E{M,x} indicates M, encrypted with key x

(a) Alice sends E{pow(g, a) mod p}, Bob replies with E{pow(g, b) mod p}
(b) Alice sends E{M2,K}, Bob replies with E{M3,K}
(c) Alice sends E{Y,K}, Bob replies with E{M,Y}
(d) None of the above protocols should be used.

14. Suppose that there is a function $f(D) = \sum_{i=1}^{n} d_i$ where each $d_i \in 0, 1$ to which we want to introduce noise. What is the sensitivity of this function?

(a) 0
(b) -1
(c) 2
(d) 1

15. GPG was originally made available to the general public by

(a) Bruce Schneier

(b) Cliffort Cox
(c) Phil Zimmerman
(d) Ron Rivest et.al.

16. Which of the following statements about PGP/GPG is *not* correct?

(a) Public keys are freely available
(b) The databases containing public keys are synchronized, stored and maintained by public key certificate authorities
(c) Secret keys are never shared
(d) Access to private keys is protected by passphrases.

17. In the way PGP is normally used, and if it is correctly used, then you can*not* verify the authenticity of a received message

(a) if it is signed by the sender
(b) if you signed the sender's public key
(c) if the sender signed your public key
(d) if the sender's public key was signed by at least 3 people whose public keys were signed by you.