سؤال القانون كان سؤال واحد , محتويات المظروف الفني بترتيب منطقي "نص الدرجة على الترتيب الأهم فالمهم" - 12 نقطة

- What is the one-time pad cryptosystem? What is it used for?
- What is the main drawback of the one-time pad?
- You can encrypt 220 values in 1 second:
    - If the key is 40 bits long:
        - How long does it take to break it?
        - Mention a scenario where it's practical, another one where it's not practical.
    - If the key is 80 bits long:
        - How long does it take to break it?
        - Mention a scenario where it's practical, another one where it's not practical.
- DES one round (**sketch**).
- Draw OFB diagram.
- Mentioned modes of operation of DES.
- Write Needham equations. What is an obvious attack against it? How to counter it?
- Needham suffers from man-in-the-middle attack, explain.
- HMAC: design goals, what is the overhead over just using a hash function, diagram
- SSL Stack Diagram.
- SSL Record Protocol operations and their security service.
- RSA Question.
- Diffie-Hellman methodology and derivation.
- Types of malicious software, their description, and whether or not they need a host.
- Diffie-Hellman problem with q=71 and alpha= 7
    - Xa=5 Xb=12 calculate Ya and Yb
- زي مسألة فاينال 2015 بنفس الارقام
- Certificate requirements.
- Contents of certificate.
- What is an Audit record? Why is it used?
- What is a Honeypot? How is it used?
- Playfair question (key = monarchy).
- How can two parties share a session key without having public keys (diagram).
- Types of intruders and their descriptions.
- Mention the two techniques for detecting intruders and their description.
- Several MCQ and True or False questions (mistakes are penalized with negative marks):
- Which of the following is reducible in GF(2):
    - X^3 + X^2 + 1
    - X^3 + 1
    - All of the above
    - None of the above
- Which 2 encryption modes permit the block cipher encryption function to be called before the data is available? **OFB & CTR**