**Principles**

* What is *confidentiality* in the context of cyber security? Your explanation must tie it to the "need to know" principle, must distinguish Eve's role from Malory's, and must point out the difference between authentication and authorization.

*confidentiality* ：information is secure,在life time中, untheorized agent cannot see, change, block it.

* **Authentication** is the process of verifying who you are. When you log on to a PC with a user name and password you are authenticating.
* **Authorization** is the process of verifying that you have access to something. Gaining access to a resource (e.g. directory on a hard disk) because the permissions configured on it allow you access is authorization.
* In the context of information security, the word *integrity* refers to three different and independent security goals. Elaborate on this and give examples of attacks against these goals.

Integrity: 保证了correctness

Modify:看了，改内容

Repudiate：看了，改source

Replay：看了，改time of issue

* Explain the Kerckhoff principle in the context of *Security By Design* versus *Security by Obscurity* and argue that it is a particularly important doctorine in an IoT environment.

 A cryptosystem should be secure even if everything about the system, except the key, is public knowledge.

**The** **Three** **Primitives**

* Explain each of the three primitives and provide examples of their applications in real-world use cases.

Symmetric: per-shared key，decry和encry用同一个key，必须meet（ASE）

Asymmetric 每个人有2个key，public和private (RSA，SSL、SSH)

Cryptographic hash function (SHA 256)

* Give an example in which the only security requirement is content integrity. Use one or more of the primitives to satisfy this requirement.

Download something from web. 只在意内容是否正确

* Can a symmetric cipher be used for authentication? For example, can it be used as an IFF (Identification, Friend or Foe) system to distiguish friendly aircrafts from enemy ones?
* Can a symmetric cipher be used for non-repudiation? For example, can it be used to make an online stock purchase (over https)?
* Digtal photographs are so easy to alter that one wonders how courts can accept them as evidence. How would you use the primitives to create a "tamper-proof seal" on digital evidence as it is collected.

**Attacks**

* How secure is a 4-digit PIN against a single-core adversary using an exhaustive attack? How about an adversary with a GPU?.
* Estimate the time needed to crack an 8-character password exhaustively on a single-core machine given that its alphabet (i.e. the set to which its chars belong) is the union of the English upper/lower case letters, the digits, and 32 symbols.

1 key/µs/core 1µs = 10^-6

Clusters can reach 1M/µsec.

* Explain the four attack categories: KCA, CCA, KPA, CPA. Which one is the most common?

Known / Chosen Ciphertext (KCA/CCA) § Known / Chosen Plaintext (KPA/CPA)

* What is the key difference between exhaustive and cryptanalytic attacks?