1 Define the 5 Cyber Security Principles.

1) Confidentiality: Ensuring that information is not accessed by unauthorized persons.
2) Integrity: Ensuring that information is not altered by unauthorized persons in a way that is not detectable by authorized users
3) Availability: Ensuring timely and reliable access to and use of information and preventing unauthorized withholding of information.
4) Authenticity: Ensuring that users are the persons they claim to be.
5) Authorization: What information is an authenticated user allowed to access or which operations allowed to perform.

2 Describe the 2 encryption models.

1) Symmetric key encryption: The encryption and decryption keys are the same. Communicating parties must have the same key before they can achieve secure communication. e.g.: AES, DES
2) Asymmetric Key encryption: The encryption and decryption keys are different, there are set of keys, private key and public key. Public key encryption key is published for anyone to use and encrypt messages. Only the party that has access to the Private key can decrypt the message. e.g.: RSA

3 Which Cyber Security Principles can be implemented via encryption?

1) Confidentiality can be implemented by both encryption models. Use DES or RSA encrypt the information to ensure it can not be accessed by unauthorized persons. The difference is asymmetric encryption methods cost much more computing resource.
2) Authorization can be implemented by asymmetric encryption methods. We can use digital signature method which implement by asymmetric encryption methods. The person who claim to be himself sign a signature encrypted by his/her private key, and we can check him by decrypt his signature using his/her public key.

4 Why we need to Root/Jailbreak a device?

Because software distribution are controlled by Apple, 3rd party developers cannot modify system components, and can only use public APIs. We need to remove certain security mechanisms to gain root privileges, patches code signing to achieve unsigned code execution and allow modifications, installation and distribution of untrusted applications by jailbreak a device.

5 Which Cyber Security Principles are compromised with Rooting/Jailbreaking a device.

1) Integrity: Jailbreak allows untrusted person modify, install applications.
2) Authenticity: Jailbreak allows patches code signing to achieve unsigned code execution.
3) Authorization: Jailbreak allows 3rd party developers gain root privilege which they should not allowed.

6 Explain, shortly, the iOS Jailbreaking process.

1) Exploit code-execution vulnerability to deploy and execute jailbreak-payload.
2) Execute payload, if required gain root by exploiting privilege escalation vulnerability.
3) Patch LLB, iBoot and Kernel to remove signature checks.
4) Install cydia to allow installation of unsigned 3rd party applications.