**Cryptography and Security Objectives**

|  |  |  |  |
| --- | --- | --- | --- |
|  | Secret key (fast) | Public key (slow) | Hash |
| Confidentiality |  |  |  |
| Integrity |  |  |  |
| Availability |  |  |  |
| Authentication (peers only) |  |  |  |
| Authentication (third party) |  |  |  |
| Non-repudiation |  |  |  |

**Cryptography and Cyber Attacks**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  | Secret key | Public key | Hash | Nonce | Time stamp |
| Passive |  |  |  |  |  |  |
|  | Eavesdropping |  |  |  |  |  |
|  | Traffic monitoring |  |  |  |  |  |
| Active |  |  |  |  |  |  |
|  | Disruption |  |  |  |  |  |
|  | Modification  |  |  |  |  |  |
|  | Fabrication  |  |  |  |  |  |
|  | Replay  |  |  |  |  |  |