Cryptography, Authentication, Identity

- Encryption vs Encoding vs Hashing vs Obfuscation vs Signing
    - Be able to explain the differences between these things.
    - Various attack models (e.g. chosen-plaintext attack).
- Encryption Standards and Implementations
    - RSA (asymmetrical).
    - AES (symmetrical).
    - ECC (namely ed25519) (asymmetric).
    - Chacha/Salsa (symmetric).
- Asymmetric vs Symmetric
    - Asymmetric is slow, but good for establishing a trusted connection.
    - Symmetric has a shared key and is faster. Protocols often use asymmetric to transfer symmetric key.
    - Perfect forward secrecy - eg Signal uses this.
- Cyphers
    - Block vs stream ciphers.
    - Block cipher modes of operation.
    - AES-GCM.
- Integrity and Authenticity Primitives
    - Hashing functions e.g. MD5, Sha-1, BLAKE. Used for identifiers, very useful for fingerprinting malware samples.
    - Message Authentication Codes (MACs).
    - Keyed-hash MAC (HMAC).
- Entropy
    - PRNG (pseudo random number generators).
    - Entropy buffer draining.
    - Methods of filling entropy buffer.
- Authentication
    - Certificates
        - What info do certs contain, how are they signed?
        - Look at DigiNotar.
    - Trusted Platform Module
        - (TPM)
        - Trusted storage for certs and auth data locally on device/host.
    - O-auth
        - Bearer tokens, this can be stolen and used, just like cookies.

    - Auth Cookies
        - Client side.
    - Sessions
        - Server side.
    - Auth systems
        - SAMLv2o.
        - OpenID.
        - Kerberos.
            - Gold & silver tickets.
            - Mimikatz.
            - Pass-the-hash.
    - Biometrics
        - Can't rotate unlike passwords.
    - Password management
        - Rotating passwords (and why this is bad).
        - Different password lockers.
    - U2F / FIDO
        - Eg. Yubikeys.
        - Helps prevent successful phishing of credentials.
    - Compare and contrast multi-factor auth methods.

- Identity
    - Access Control Lists (ACLs)
        - Control which authenicated users can access which resources.
    - Service accounts vs User accounts
        - Robot accounts or Service accounts are used for automation.
        - Service accounts should have heavily restricted priviledges.
        - Understanding how Service accounts are used by attackers is important for understanding Cloud security.
    - impersonation
        - Exported account keys.
        - ActAs, JWT (JSON Web Token) in Cloud.
    - Federated identity