Encription

- Database
  - Encript before add, decript after get
    - Cannot prevent table structure from leaking
    - Create problem during query database
  - SQLCipher

MD5

- Hash function
- Any data --> same length
- Eazy to cal MD5
- Change small, big difference
- Hard to have same MD5 from different data
- Cannot revert
- Scenarios:
  - Password verify
  - File check

RSA

- Asymmetric encryption
- Data encrypted with the public key can only be decrypted by the paired private key
- Limitation on the length of the encrypted data: key.length-11
  - To encrypt longer data: segment encryption and decryption
- Scenarios 1:
  - (1) Android create Keypair by KeyPairGenerator
  - (2) Android use PublicKey to encrypt data and save locally
  - (3) Android use PrivateKey to decrypt the data and send it to Server
    - eg: Work with Android FingerprintManager.authenticate
- Scenarios 2:
  - (1) Server create Keypare
  - (2) Server send PublicKey to Android
  - (3) Android use PublicKey to encrypt data
  - (4) Server use PrivateKey to decrypt data
- Scenarios 3:
  - (1) Android create Keypair by KeyPairGenerator
  - (2) Android send the PublicKey to Server
  - (3) Android save the data
  - (4) Android use a Signature (initailized by PrivateKey and sign with the data), and sent signtureBytes to Server
  - (5) Service use a Signature (initailized by PublicKey and update with original data), and verify the signtureBytes.

AES

- Symmetric cipher
- Same key is used for encryption and decryption
- Key length support: 128, 192, 256 Key
- Create Key by KeyGenerator, or using any 16, 24, 32 bit String