Cryptography on Android

with Keisler Dharmawan

Covering...

- What's Cryptography?
- Android and Cryptography
    - Involved Classes
- Encryption Methods
- Demonstration/Lab

Cryptography

- Hide information
- Securing information
- Achieved by algorithms
- Popular methods of encryption
    - AES (symmetrical, 1 private key)
    - DES (symmetrical, 1 private key)
    - RSA (asymmetrical, 1 private, 1 public key)
- Text or Data

Android Cryptography

- Supports all encryption methods
- Uses Crypto package
- includes classes Crypto.
    - Cipher
    - KeyGenerator
    - SecretKey
    - spec.SecretKeySpec
- Requires... (for example)
    - Plain Text
    - Key
    - Desired Encryption Method

Cipher Class

- Used to specify an encryption method by specifying its instance.
- Usage: Cipher c = Cipher.getInstance("x");
- Where x can be "algorithm/mode/padding" or just "algorithm"
- Example:

```
Cipher c = Cipher.getInstance("AES/CBC/PKCS5Padding");
```

KeyGenerator Class

- Works together with SecureRandom and SecretKey classes
- Creates a specific AES/DES keys for its implementations
- Maximum key length

  AES = 128 bits
  DES = 64 bits

SecretKeySpec Class

- Generated keys made by KeyGenerator used to create the secret key for both AES and DES
- The secret key is then used for encryption and decryption

How to Encrypt

1. Turn Key into raw key form according to the method of encryption.
2. Initialize the AES encryption specification
3. Configure keys
4. Start encrypting plaintext

How to Decrypt

- Same method as Encrypt, with different parameter.
- Cipher.DECRYPT_MODE instead of Cipher.ENCRYPT_MODE

Demo Code

http://tinyurl.com/64wmkgo