Cryptography

Group # 6

<Students’ names redacted>
Topics

- Overview of Encryption
- History of Encryption
- Types of Encryption
- Problems and Solutions
- How the Code Works
- Demonstration of App
Overview of Encryption

- Why use Encryption?
- Other uses of Encryption
- Why SMS Encryption
History

- 36th Century – Egyptian hieroglyphs
- 1834 – Samuel Morse develops Morse Code
- 1917 – Zimmermann telegram intercepted and decrypted

- 1976 – Data Encryption Standard (DES) published as a standard for the US
  - 56-bit key
  - Symmetric key algorithm
  - Criticized for key being too short and using classified design elements
  - Motivated modern understand of cryptanalysis

- Public Key Cryptography
  - Asymmetric key algorithm
  - Used in Transport Layer Security (TLS), Pretty Good Privacy (PGP), and GNU Privacy Guard (GPG)

Types

- Symmetric
  - Stream Ciphers
  - Block Ciphers
- Asymmetric
- Hash Functions

A) Secret key (symmetric) cryptography. SKC uses a single key for both encryption and decryption.

B) Public key (asymmetric) cryptography. PKC uses two keys, one for encryption and the other for decryption.

C) Hash function (one-way cryptography). Hash functions have no key since the plaintext is not recoverable from the ciphertext.

http://www.garykessler.net/library/crypto.html
Symmetric

- Uses same key to encrypt and decrypt
- Stream cipher – encrypt bits one at a time
  - Self-synchronizing
  - Synchronous
- Block cipher – encrypt a number of bits as a single unit
  - Modes:
    - Electronic codebook
    - Cipher-block chaining
    - Cipher feedback
    - Output feedback

http://www.garykessler.net/library/crypto.html
Asymmetric

- Public Key Cryptography
- Public key used to encrypt
- Private key used to decrypt
- Relies on one-way functions
- Two keys are related, but knowing one key does not give away the other
- Digital signatures

http://www.garykessler.net/library/crypto.html
Hash Function

- One way encryption
- Takes a block of data, returns a fixed-size bit string (hash value)
- Data to be encrypted called the message
- Hash value called the digest
- 4 main properties
- Uses

http://www.garykessler.net/library/crypto.html
Problems Faced

- Encryption issues
- Copying message from SMS
- Installing and using Windows 7 Phone development tools
Encryption Method

- Original Method – Pre-Encryption Lecture
  Encrypt: \((\text{ASCII Value} + \text{Pin}) \mod 127\)
  Decrypt: \((\text{ASCII Value} - \text{Pin}) \mod 127 + 127\)

- Issues – String truncation

- Solution – Post-Encryption Lecture
  XOR: Encrypt/Decrypt: \((\text{ASCII Value} \ XOR \text{PIN})\)
Copying Text Received from SMS

- Problem – Get Text from Message to App
- Possibilities
  - Insert a link in the message
    - Unsupported
  - Host our own Messaging Server
    - Not enough resources
  - Use Copy/Paste Functionality
    - Cheap way out, but only solution
Copying Text Received from SMS

- Why not a link to our App?
  - Security Issues for Windows 7 Phone
  - Potentially will be opened up in future
  - IPhone and Android Development Tools allow this method of launching an App
- Decided to use Copy/Paste
Installing and using Windows 7 Phone development tools

• Simple Setup
  • Install Visual Studio 2010
  • Install Windows 7 Phone Development Tools
  • Create Windows 7 Phone Project
  • Write Code
  • Run in Emulator
Windows 7 Phone Development

• Microsoft Visual Studio
  • Main tool used
  • Easy Drag/Drop GUI

• Expression Studio 4
  • Easy GUI creation tool
Code Hierarchy

- App
- MainPage
- PinInput
PinInput - Navigation

- **private void button1_Click (object sender, RoutedEventArgs e)**
  - `this.NavigationContext.QueryString["Mode"] == "Encrypt"`
PinInput

- private string Encrypt(int pin, string text)

- private string Decrypt(int pin, string text)
Windows Phone Launchers and Tasks

- Provided namespace
  - Allows execution of common tasks
- SMSComposeTask
  - Launches texting interface
Our App

- Demo
Summary

- Reasons for Encryption
  - Protecting secure messages from threats, attacks, and people
- History of Encryption
- Type of Encryption
  - Symmetric
  - Asymmetric
  - Hash Function
- Problems and Solutions
- How The Code Works
- Demonstration