Network Security

Symmetric Key Cryptography

Today

- Substitution Ciphers
- Transposition Ciphers
- Cryptanalysis

Crypto as Munitions

- Does:
  - protecting information kill enemies?
  - failure to protect information kill friends?
  - failure to "steal" enemy information kill friends?
- US Government decided that enough of the above were "yes" to declare crypto munitions

Crypto as Munitions

- Why are export restrictions a problem?
  - Commercial applications of strong cryptography abound
  - US Corporations cannot export products that use strong cryptography
  - Foreign companies will take the market for crypto applications and all that goes with it

History of Cryptography

- Primary use: Military
- Romans (probably before)
- WWII (Ultra, Enigma, Japanese unbreakable codes)
- Data Encryption Standard
- Public Key Cryptography

History of Cryptography

- Substitution ciphers
- Transposition ciphers
- Codes
- Combinations
Substitution Cipher

- bmddmg replacement
- Each letter is replaced by another letter

- Caesar cipher
  PLAINTEXT  a b c d e f g h i j k l m n o p q r s t u v w x y z
  CIPHERTEXT D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

- Rot13
  PLAINTEXT  a b c d e f g h i j k l m n o p q r s t u v w x y z
  CIPHERTEXT N O P Q R S T U V W X Y Z A B C D E F G H I J K L M

- Twenty six letter key
  PLAINTEXT  a b c d e f g h i j k l m n o p q r s t u v w x y z
  CIPHERTEXT Random selection of order

Transposition Cipher

a l b k a s b l t e
b a s k e t b a l l

Transposition Ciphers

- Word embcrals
- Key = 7523461
- Blocks

```
 1 2 3 4 5 6 7  7 5 2 3 4 6 1
 t h i s i s a i h i s s t
 n e x a m p l i m e x a p n
 e o f a t r a a t o f a r e
 n s p o t i o o t s p i o n
 n c i p h e r r h c i p e n
```

Codes

- Words/phrases are substituted with other words, phrases, or numbers
- Code books are required.
- Advantages/disadvantages
Codes

- Attack
- Retreat
- Defend
- Defend at all costs
- Surrender
- Sunrise
- Sunset
- Rain
- Snow
- Notinyourlifetime

Substitute, Transpose, Codes

- Unbreakable Japanese code in WW II
- Combination is foundation of modern crypto

Cryptography Paradigms

- Symmetric Key Cryptography
  - Private/Secret Key Cryptography
  - Encrypt/decrypt with the same key
- Asymmetric Key Cryptography
  - Public/Private Key Cryptography
  - Encrypt/decrypt with different keys
- Hash: Creates a message digest
- Signature: Foundation of non-repudiation

More Cipher Techniques

- Reverse Cipher
- Railfence Cipher
- Syctale Cipher
- Geometric Figure
- Nilhilist Cipher
- Feistel Structures

Reverse Cipher

- Reverse the order of the letters in a message.
- egasemanisrettelehtforedroehthesrever

Rail Fence Cipher

- Write the message alternating letters in two rows
  
  ```
  w i e h m s a e n w r w
  r t t e e s g i t o o s
  ```

  Write the ciphertext from the rows
Scytale Cipher
- An early Greek transposition cipher
- A strip of paper was wound round a staff message written along staff in rows, then paper removed leaving a strip of seemingly random letters

Nihilist Cipher
- Combines row and column transposition
- Write message in rows in order controlled by the key
- Read off by rows, but in order controlled by the key
- Plaintext: NOWISTHETIMEFORALLGOODMEN

\[
\begin{array}{cc}
1 & 2 & 3 & 4 & 5 \\
1 & 2 & 3 & 5 & 4 \\
\end{array}
\]

Plaintext: NOWISTHETIMEFORALLGOODMEN

Ciphertext: HTEIT ONWSI EMFRO DOMNE LALOG

Product Ciphers
- Ciphers based on just substitutions or just transpositions are not secure
  - Two substitutions are really only one more complex substitution
  - Two transpositions are really only one more complex transposition
- What about when we combine the two?
  - Substitute
  - Transpose
  - Substitute
  - Transpose
  - Etc.

Machine Ciphers
- Jefferson cylinder

Machine Ciphers
- Wheatstone Disc

Enigma Rotor machine
- It allowed encryption of a large volume of data
- Utilized several wheels (rotors) placed adjacent to one another. Each performed a monoalphabetic substitution.
- Similar to a "souped up" Vigenere cipher
Stream Ciphers

- Data is encrypted a bit or byte at a time
- **Confusion sequence** is created at encryption time and is combined with the plaintext to form the ciphertext stream.
- The key allows recreation of the confusion sequence for recreation of the plaintext at the receiving end

Confusion Sequence

- Random Number Stream
  - Generate one random bit at a time & XOR
  - One time pad, with all its up and down sides
- Substitution Cipher
  - Substitute a byte at a time
- Keyed Random Number Generator
  - Use the same RNG and the same IV ⊕ key

One Stream Cipher

- Parties share key k.
- RC4 is a random number generator that deterministically generates a string of random bits given two parameters
- An initialization vector is created by the originator
- CT = PT ⊕ RC4(IV, k)
- Transmit (CT,IV)

Stream Cipher with RC4

<table>
<thead>
<tr>
<th>Plaintext</th>
<th>CRC</th>
</tr>
</thead>
<tbody>
<tr>
<td>⊕</td>
<td></td>
</tr>
<tr>
<td>RC4 (v,k)</td>
<td></td>
</tr>
<tr>
<td>v</td>
<td>Ciphertext</td>
</tr>
<tr>
<td>⊕</td>
<td></td>
</tr>
<tr>
<td>RC4 (v,k)</td>
<td></td>
</tr>
<tr>
<td>Plaintext</td>
<td>CRC</td>
</tr>
</tbody>
</table>

Review

- Substitution Ciphers
- Transposition Ciphers
- Stream Ciphers