Jan 26, 2005 -- Lecture 4

22C:169 Computer Security

Douglas W. Jones

Department of Computer Science

From Caser to 1920

An example Caesar Cypher

Plaintext: **`The quick brown fox`**
`jumps over the lazy dog`

Key: **`abcdefghijklmnopqrstuvwxyz`**
`efghijklmnopqrstuvwxyzabcd`

Cypher: **`Xli uymgo fvsar jsb`**
`nyqtw sziv xli pedc hsk`

Cracking the Example

Cypher: **`Xli uymgo fvsar jsb`**
`nyqtw sziv xli pedc hsk`

Frequencies: 4{**`s`**} 3{**`i`**} 2{**`xlvy`**}

English Frequency: **`etaoin shrdlu`**
The common word: **`the`**

Try:
```
abcdefghijklmnopqrstuvwxyz
    ....e  h       ....t
```

Conclusion: it was Rotate 4!

Strengthen the Code

Idea: Change rotation after each letter

Plaintext: **`The quick brown fox`**
`jumps over the lazy dog`

Tool: **`abcdefghijklmnopqrstuvwxyz`**
`[                          ]`

Cypher: **`Xmk xcrmv necld wgq`**

What form does the key take?

initial rotation

rotation after encrypting each letter

t	efghijklmnopqrstuvwxyzabcd
h	fghijklmnopqrstuvwxyzabcde
e	ghijklmnopqrstuvwxyzabcdef
q	hijklmnopqrstuvwxyzabcdefg
u	ijklmnopqrstuvwxyzabcdefgh
i	jklmnopqrstuvwxyzabcdefghi
c	klmnopqrstuvwxyzabcdefghij
k	lmnopqrstuvwxyzabcdefghijk
b	mnopqrstuvwxyzabcdefghijkl
r	nopqrstuvwxyzabcdefghijklm
o	opqrstuvwxyzabcdefghijklmn
w	pqrstuvwxyzabcdefghijklmno
n	qrstuvwxyzabcdefghijklmnop
f	rstuvwxyzabcdefghijklmnopq
o	stuvwxyzabcdefghijklmnopqr
x	tuvwxyzabcdefghijklmnopqrs

Double Encryption

The idea:

Encrypt the message once
Then encrypt it again

The hope:

We could double the key size

The reality: these two are equivalent

Rotate A Step D || *Rotate B Step E*
Rotate A+B Step D+E

What about arbitrary permutation?

Double encryption is worthless

What if we rotate after each letter?

Double encryption begins to work!

Rotor machines:

The rotor encodes a permutation

After each letter, the rotor turns

Multi-rotor machines:

The rotors work like an odometer

The Enigma