EECS 1001 RESEARCH DIRECTIONS IN COMPUTING

YORK UNIVERSITY

A BRIEF ENCOUNTER WITH

INFORMATION SECURITY

PROF H ROUMANI
EECS, York University

INFOSEC

From Biology to Computing to Physics, it's all about:

INFORMATION

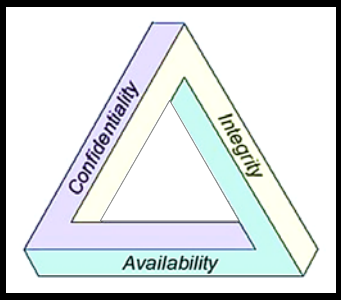
2

INFOSEC

- *As such, you want to make sure that information is secure.*
- *Throughout its lifetime and wherever it is: in storage, processing, or transit.*
- *Unauthorized agents should not be able to see it, change it, or block it.*

3

THE CIA TRIAD



4

PRINCIPLES

- Confidentiality
  Based on authentication and authorization
- Integrity
  Of content, source, and time of issue
- Availability
  Anytime, anywhere to authorized users

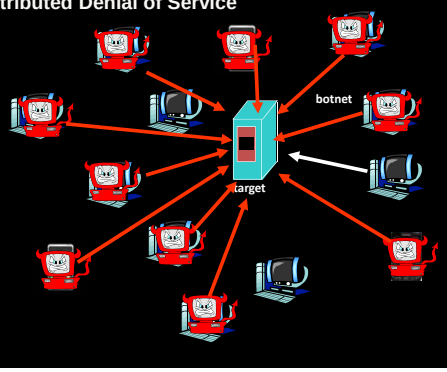
ATTACKS

- SPY
- DIVULGE
- MODIFY
- REPUDIATE
- REPLAY
- BLOCK
- D-DOS

5

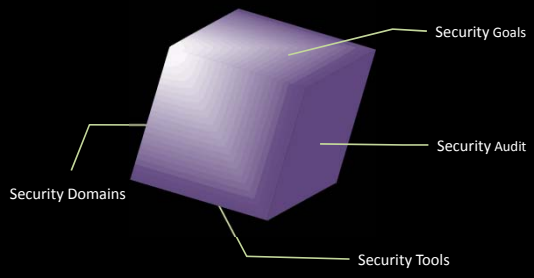
D-DOS

Distributed Denial of Service



6

FACADES



The Computer Security Honours Program @York

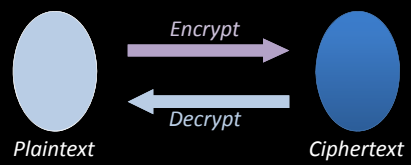
7

CRYPTO

1. Steganography
2. Symmetric Ciphers
3. Public Key Crypto
4. Cryptographic Hash Functions
5. Quantum Key Distribution

8

TERMINOLOGY



9

Symmetric Ciphers

1. Alice and Bob meet in person
2. They agree on a secret key K
3. They then part ways.

When Alice wants to send something to Bob

1. She encrypts in with K
2. And sends the ciphertext to Bob
3. Who uses K to decrypt.

Most popular: **AES**

10

Caesar

Mono-Alphabe

The key is 3

Plaintext

```
THE KEY OF THIS CODE SHIFT IS THREE
WKH NHB RI WKLV FRGH VKLIW LV WKUHH
```

Ciphertext

```
Encrypt:  c = (p + k) % 26;
Decrypt:  p = (c - k) % 26;
```

Can you attack it?
Exhaustively?
Analytically?

A	0
B	1
C	2
D	3
E	4
F	5
G	6
H	7
I	8
J	9
K	10
L	11
M	12
N	13
O	14
P	15
Q	16
R	17
S	18
T	19
U	20
V	21
W	22
X	23
Y	24
Z	25

11

Exhaustive Key Space Scanning

Key size (bits)	Number of possible keys	decryptions per µs 1	10^6
5	$2^5 = 32$	32 µs	
32	$2^{32} = 4.3 \times 10^9$	1 hr	2.15 ms
56	$2^{56} = 7.2 \times 10^{16}$	10^3 yr	10 hr
128	$2^{128} = 3.4 \times 10^{38}$	10^{24} yr	10^{18} yr
168	$2^{168} = 3.7 \times 10^{50}$	10^{36} yr	10^{30} yr

The age of the universe is only ~13.6 billion years

12

Stats for English (Cryptanalytic Attacks)

- **Monogram**
  E (13%), T (9%), A (8%)
  O, N, R, I, S, H — 6%
  D, L — 4%
  F, C, M, U, G, Y, P, W — 2%
  B, V, K — 1%
  X, J, Q, Z
- **Bigram**
  TH, HE, AN, RE, ER, IN, ON, AT, ND, ST, ES, EN, OF, TE
- **Same-letter Bigram**
  LL, EE, SS, OO, TT, FF, RR, NN, PP, CC, MM, GG
- **Trigram**
  THE, ING, CON, ENT, ERE, ERS, EVE, FOR, HER, TED, TER, TIO, VER

13

VIGENÈRE

Poly-Alphabetic

The key is YORK

Plaintext

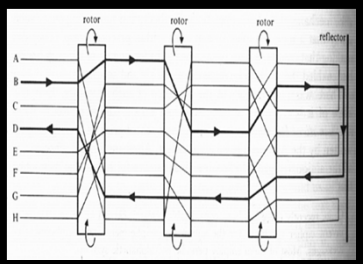
```
AT THE START OF THE FIRST GAME THE
YO RKY ORKYO RK YOR KYORK YORK YOR
YH KRC GKKPH FP RVV PGFJD EODO RVV
```

Ciphertext

Can you attack it?

14

THE ENIGMA



15

Public Key (aka Asymmetric)

Problem with Symmetric Crypto: Alice and Bob must first meet in person. E-commerce can't work like this!

- Bob chooses two keys: a public and a private
- Given the public key, finding the private is as hard as factoring a large integer
- Can encrypt with either, decrypt with the other
- Alice encrypts with Bob's public
- Most popular: RSA

16

Factoring is Hard

What are the factors of: [100 digits]

1522605027922533360535618378132637429718068114961380688657908494580122963258952897654000350692006139

They are: [50 digits]

3797522793694367392280887275544562785456553663819 9

and: [50 digits]

4009469095092088103068373529276146838921489972406 1

See http://en.wikipedia.org/wiki/RSA_numbers#RSA-100

17

Public Key Examples

- I know Amazon's public key
- I use it to encrypt my order and send the ciphertext
- Only Amazon can decrypt

➔ Confidentiality w/o a prior in-person meeting!

- Amazon encrypts a warranty with its private key
- And sends the ciphertext to me
- I decrypt it with its public key

➔ And so can others but Amazon cannot repudiate!

18