The CS 5 Times

Penguin Rescue!

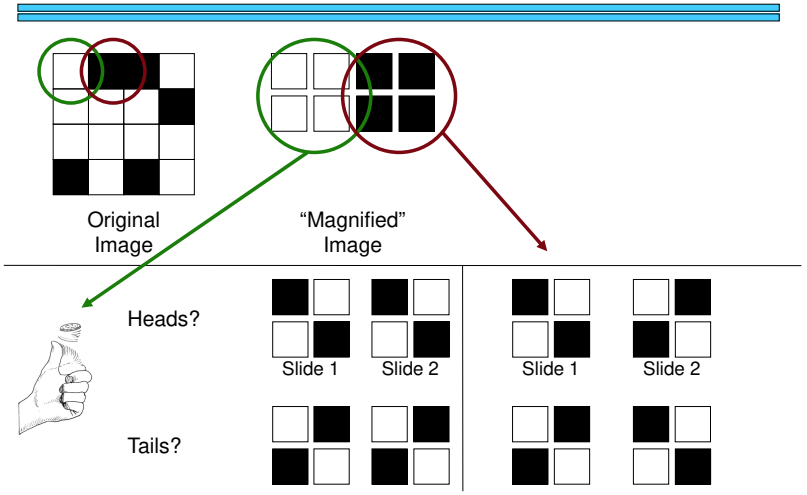
Dunedin, New Zealand (Penguin Press):

A daring mission has been mounted to rescue two adorable penguins who had been given up as lost after a spaceship crash. Risking her life with an untested experimental jet pack, a brave Chemistry penguin mixed a witches' brew of propellant, fueled the pack, and set off across the sky in search of her missing colleagues, who were running out of fish when last heard from.

"We are, like, so grateful for this, like, attempt, and, like, we, like, hope for her, like, success," stated a jittery CS 5 student. "We like, love our, like, penguins and are, like, so helpless with our, like, homework assignments without, like, their, like, help."

Further quotes were unavailable due to an unexpected attack from a WRIT 1 instructor.

Secret Sharing…



Cryptography!

Spartan scytale (500 BCE)

Caesar Cipher (100 BCE)

```
"senddonuts"
     |
     ↓
"vhqggrqtwv"
```

Symbols ←→ Numbers

Symbol	Number
' '	32
!	33
…	
.	46
…	
A	65
B	66
…	
Z	90
a	97
b	98
…	
z	122

```
>>> ord('A')
65
>>> ord('!')
33
>>> chr(65)
'A'
>>> chr(33)
'!'
```

Symbols ←→ Numbers ←→ Binary Strings

Symbol	Number	Binary String
' '	32	'00100000'
!	33	'00100001'
…		
.	46	'00101110'
…		
A	65	'01000001'
B	66	'01000010'
…		
Z	90	'01011010'
a	97	'01100001'
b	98	'01100010'
…		
z	122	'01111010'

XOR

	A	B	A XOR B
0 XOR 0 = 0	0	0	0
0 XOR 1 = 1	0	1	1
1 XOR 0 = 1	1	0	1
1 XOR 1 = 0	1	1	0

Associative: `(0 XOR 1) XOR 0 = 0 XOR (1 XOR 0)`
Commutative: `0 XOR 1 = 1 XOR 0`

What is `0 XOR 1 XOR 1 XOR 0 XOR 1`?

What is `x XOR y XOR x`?

Worksheet!

XOR

	A	B	A XOR B
0 XOR 0 = 0	0	0	0
0 XOR 1 = 1	0	1	1
1 XOR 0 = 1	1	0	1
1 XOR 1 = 0	1	1	0

One-time pad

`00111101 01111010 00010011 …`

One-time pad images from www.ranum.com and www.home.egge.net

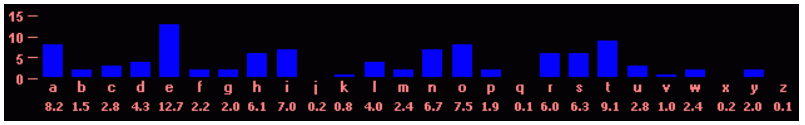
Encoding and Decoding

Original Message:		I	space	h …
Binary Version:		01001001	00100000	01101000
One-time pad:		00111101	01111010	00010011
	XOR			
Encrypted:		01110100	01011010	01111011
In text form:		t	Z	{

Encoding and Decoding

Original Message:		I	space	h …
Binary Version:		01001001	00100000	01101000
One-time pad:		00111101	01111010	00010011
	XOR			
Encrypted:		01110100	01011010	01111011
One-time pad:	XOR	00111101	01111010	00010011
Original Message!		01001001	00100000	01101000
		I	space	h …

Letter Frequencies



Histogram courtesy of http://www.simonsingh.net/The_Black_Chamber

What's the "One Time" Part?

Tuesday's message:

ATTACK AT DAWN => HBWAKYBYAVLMQ4

Wednesday's message:

RETREAT AT TEN => [SWRMS68T"(XC4

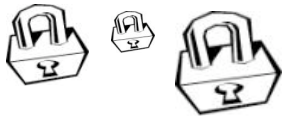
Tuesday XOR Wednesday:

Not printable, but the one-time pad drops out!

Alice, Bob, and their Locks

Alice

Bob



How Does This Help Us?

Alice

Pad_{Alice}

Bob

Pad_{Bob}

How Does this Help Us?

((Pad$_{Alice}$ XOR Message) XOR Pad$_{Bob}$) XOR Pad$_{Alice}$) = Message XOR Pad$_{Bob}$

Alice

Pad_{Alice}

Bob

Pad_{Bob}

How Does this Help Us?

(Message XOR Pad$_{Bob}$) XOR Pad$_{Bob}$ =?

Alice

Pad_{Alice}

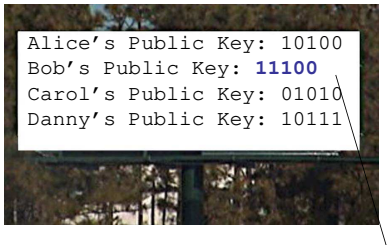
Bob

Pad_{Bob}

This seems like a great trick but…

Worksheet!

Public Key Cryptography!



`f` is public and used by all parties!

Alice (Private Key: 010110)

"I like spam"

↓

10110100010

↓

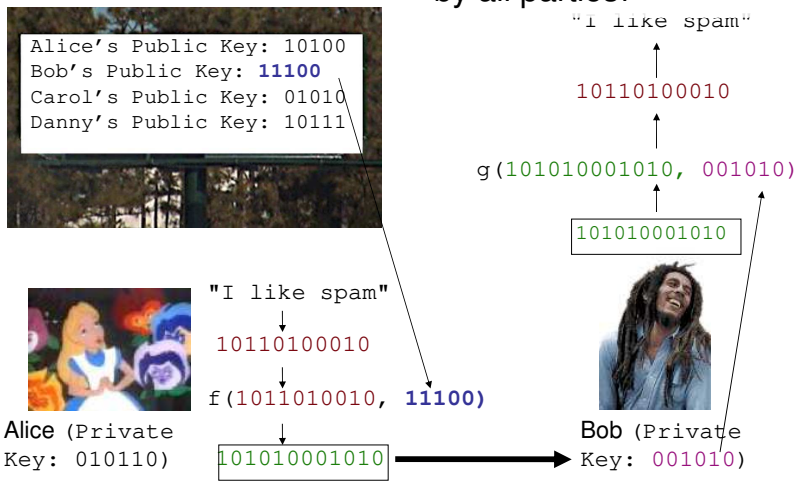
f(1011010010, **11100**)

↓

101010001010

Bob (Private Key: 001010)

Public Key Cryptography



Cryptographic Hashes

```
def badhash(s):
  x = sum([ord(c) for c in s])
  return x % 1009

>>> badhash("hello")
532
>>> badhash("hello there")
91
```

Cryptographic Hashes

```
def sha1(s):
   x = # much magic
   return x

>>> sha1("hello")
f572d396fae9206628714fb2ce00f72e94f2258f
>>> sha1("hello there")
55e82e1eb131597ce6ef77ff775b2c2e5f4d6b45
```

Digital Signatures

```
message = "Pay $1M to SAT proctor"
hash = sha1(message)
proof = encrypt(hash, felicity_private_key)
secret = encrypt(message + proof,
   bank_public_key)

send(secret)
```