



Computer Science 50

Introduction to Computer Science I

Harvard College

Week 2

David J. Malan
malan@post.harvard.edu

Or fher gb qevax lbhe binygvar!

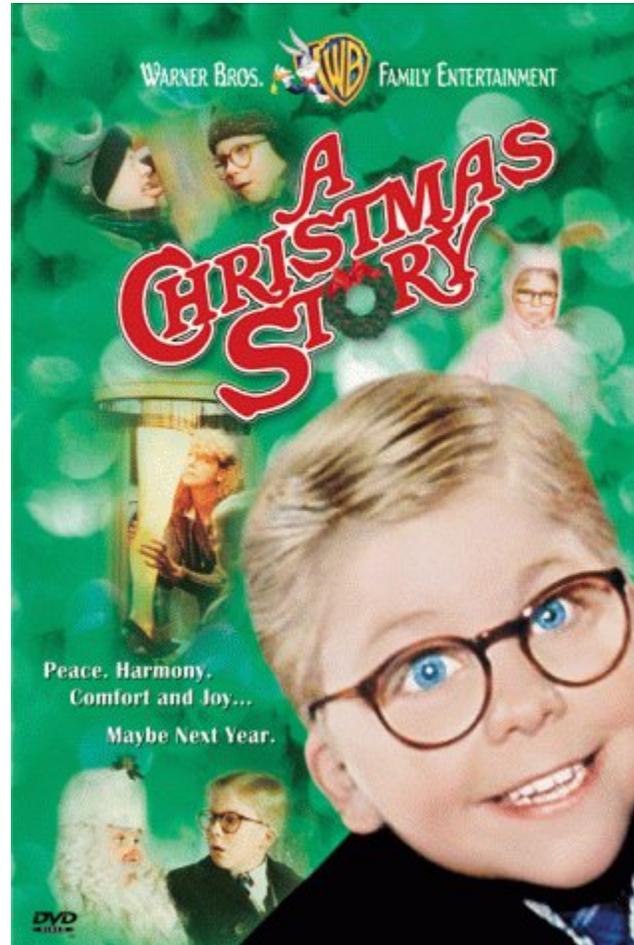


Image from <http://www.questexperiences.com/quest2/movieadventures/default.asp>.

How to Write a Program in...

- :: C++
- :: Java
- :: LISP
- :: Perl
- :: PHP
- :: ...

see
`hai.{cc,lisp,php,pl}, Hai.java`

Bugs

Photo # NH 96566-KN First Computer "Bug", 1945

92

9/9

0800 Antam started
1000 " stopped - antam ✓
13⁰⁰ (033) MP-MC ~~1.98264000~~ { 1.2700 9.037 847 025
 (033) PRO 2 2.130476415 } 9.037 846 995 connect
 connect 2.130676415
Relays 6-2 in 033 failed special speed test
in relay .. 11.00 test.

1100 Started Cosine Tape (Sine check)
1525 Started Multy Adder Test.

1545  Relay #70 Panel F
(moth) in relay.

1630 Antam started.
1700 closed down.

Relay 3145
Relay 3376

First actual case of bug being found.

see
buggy{1,2}.c

Casting

```
int i = (int) 'A';  
char c = (char) 65;
```

see
`ascii{1,2,3}.c, battleship.c`

Functions

Parameters and Arguments

99 bottles of beer on the wall,
99 bottles of beer,
Take one down, pass it around,
98 bottles of beer on the wall.



see
`beer{1,2,3,4}.c`

Functions

Scope, Local Variables, Temporary Variables

```
void  
swap(int a, int b)  
{  
    int tmp;  
  
    tmp = a;  
    a = b;  
    b = tmp;  
}
```

see
buggy3.c

Functions

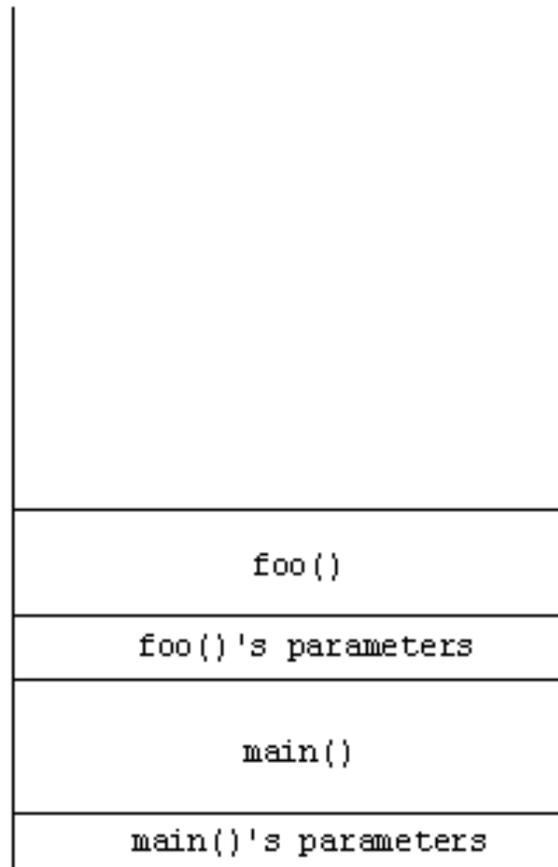
Scope, Global Variables

```
void  
increment()  
{  
    x++;  
}
```

see
buggy4.c, global.c, buggy5.c

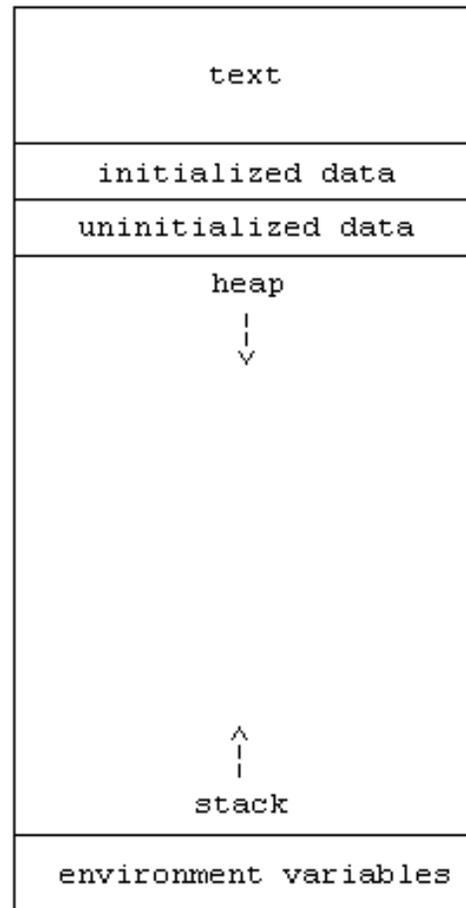
The Stack

Frames



Memory Management

Sneak Preview



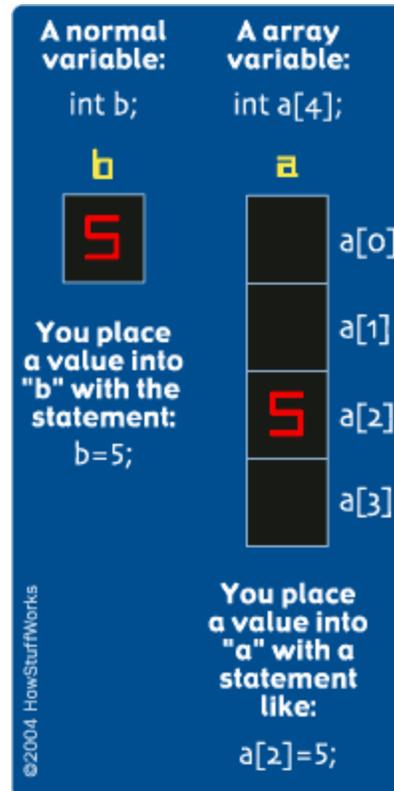
Functions

Return Values

```
int  
cube(int a)  
{  
    return a * a * a;  
}
```

see
`return{1,2}.c`

Arrays



see
`array.c`, `buggy6.c`, `string{1,2}.c`, `capitalize.c`

Free Resources

<http://www.howstuffworks.com/c.htm>

<http://www.cppreference.com/>

Command-Line Arguments

`argc, argv`

```
int main(int argc, char *argv[]);
```

see
`argv{1,2}.c`

CS 50's Library

(Memory Leaks)

```
:: bool
:: string

:: char GetChar();
:: double GetDouble();
:: float GetFloat();
:: int GetInt();
:: long long GetLongLong();
:: string GetString();
```

see
<http://cs50.net/pub/releases/cs50/>

Cryptography

Or fher gb qevax lbhe binygvar!



Cryptography

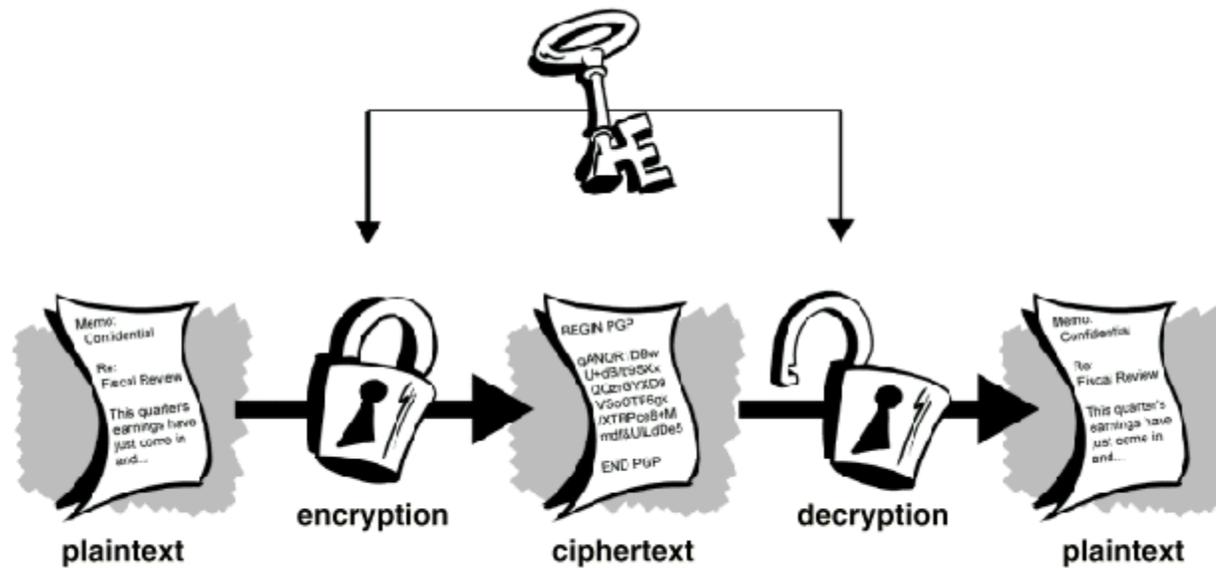
Enigma Machine



Image from http://en.wikipedia.org/wiki/Enigma_machine.

Cryptography

Secret (Symmetric) Keys



Cryptography

Caesar Cipher

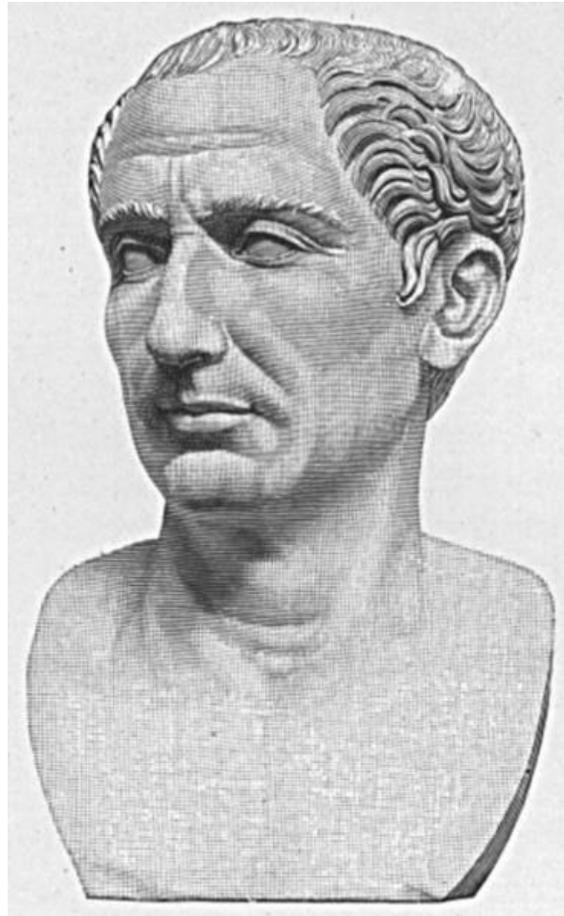
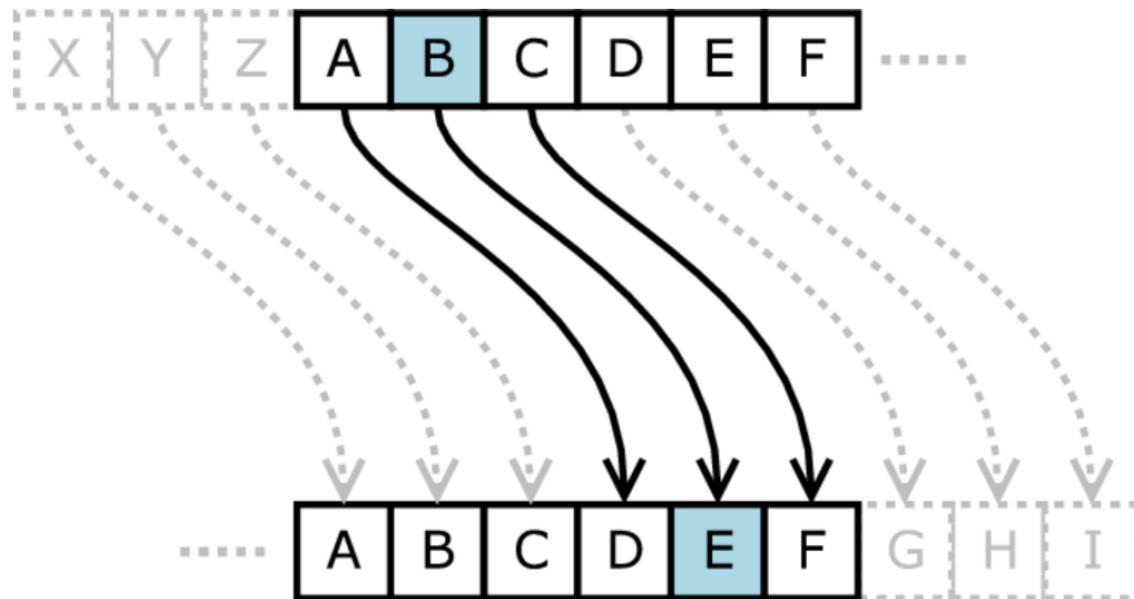


Image from <http://commons.wikimedia.org/wiki/Image:Hw-caesar.jpg>.

Cryptography

Caesar Cipher

$$c_i = (p_i + k) \% 26$$



Cryptography

Vigenère Cipher

$$c_i = (p_i + k_i) \% 26$$

<i>p</i>	H	E	L	L	O	,	W	O	R	L	D
	+	+	+	+	+		+	+	+	+	+
<i>k</i>	F	O	O	B	A		R	F	O	O	B
	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
<i>c</i>	M	S	Z	M	O	,	N	T	F	Z	E

Cryptography

DES

72,057,594,037,927,936

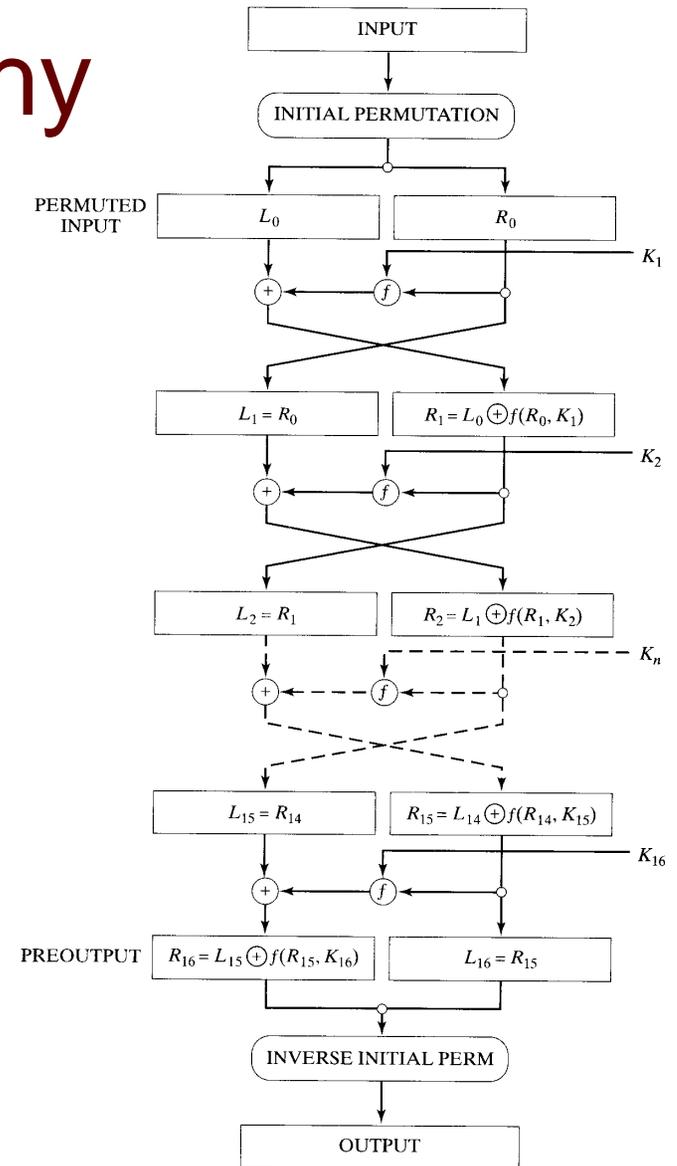
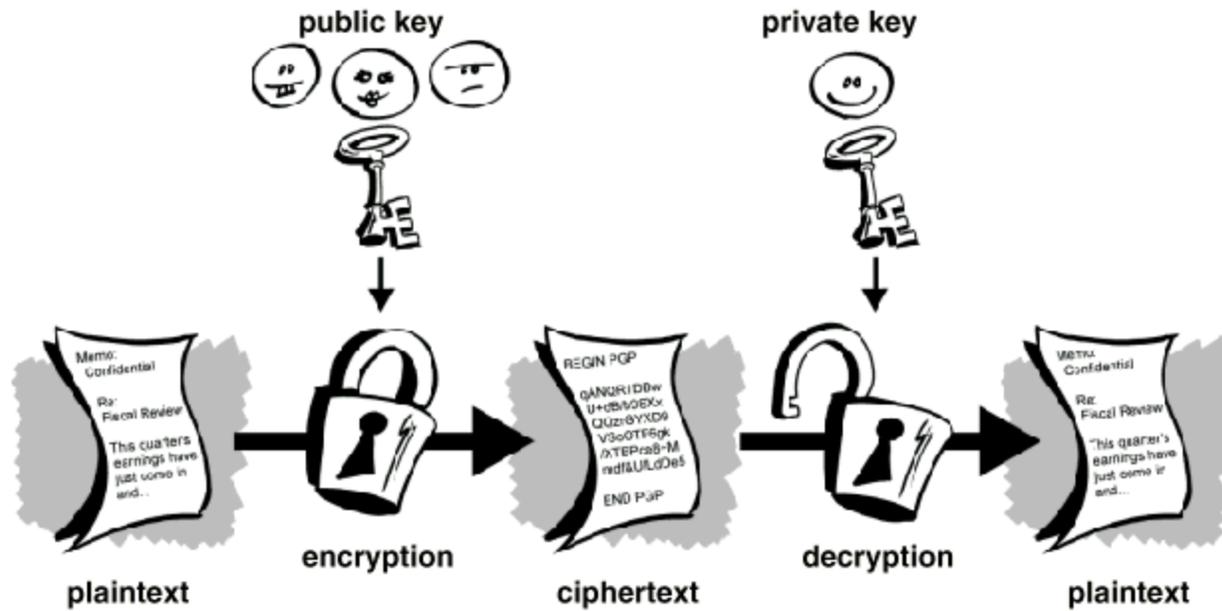


FIGURE 3-14 DES.

Cryptography

Public and Private (Asymmetric) Keys



Cryptography

PGP

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGP Key Server 0.9.6

```
mQGIBEFMqoURBADaifCKsYkPBmVSMvspdLHLIAsb0xe4cyOieCA5LQCUZi9Z+Yxu
OSMkbQ+VSAvtP31/7o9pNf6LsLU4ADA5knZVB+GfZZpiGnEd62qKDKNpjVo20NRH
Xcd/4RpxE6aJWUWe2tPqLSCi3NFLPEhfnfo5v9WyLRHjqdIQKc6vGAT41BQCg/5/1
vNpKhyA6VrFDIuozNWqKpAUD/11AHxPxfLyn8K/Gv/w10y97dRDq0vsRqkh57IT
YKy/Xjv4qzNWZ/dSXI7Fa/6xULRuYK6tcr5aI6bFVVL14fIXn5tapcCdYLAMo2ap
Uf/+PRJgSNUg4j50F5GjjiKco7FY1daF3oy6DVQzjEtSHN2TFczVOMHJUax1Ip/U
DRjIA/9vOO/MZ7FspAW1ZOdC13CxVSnig4oALGbnf76RviFG010bByVLV1BxMi1L
v8wxSbydqxsvokPZ/ucOfSqedO+l9xmIEp/Luq4k2owKfyAB2U33+HkfkzS8RM4zJ
Wyl18jXNzEfyFsqmJ0RKfzJe7jXX34ZMfbPc3r39eR4w91o+bQmUm9uYWxkIEWg
Uml2ZXN0IDxyaXZlc3RAY3NhaWwubWl0LmVkdT6JAEYEEBECAAYFAkFMquoACgkQ
5DGedS1eYN7UGACgzEZmCLhzVz2kc3/5curi183AiMAN3NOJx6SJOL3n2fNAaar
7B5M0z9ZiQBBBARAgAGBQJBTK1BAAoJEKXuoAZz/b3Wi9oAoPYpdchyMlydUjzh
GxiwYxQEzS8uAJ91BLfy5FIIGYlgHz/QkcUS+Ps2N4kAVAQQEQIAFAUCQYyqhQUU
AmpPgaQLAwIBAhkBAoJEIIdenepUv6CUvGQAoKNCAjxfDnc1/Lf73xvQLq//YBRt
AKC15mvYi3D+w+4NikexCA+tQe9korkEDQRBTkqFEBAA+RigflogYXpDkXcBWyH
huxh7M1Fhw7Y4KN5xsncigus5D/jRpS2MEpT13wCFkiAtRX1LKZmpnwd00//jocWW
IE6YZbjYDe4QXau2FxxR2FDK1ldDKb6V6FyrOHhcC9v4TE3V46pGzPvOF+ggnRRh
44SpT9GDhKh5tu+Pp0NGCmbMHXdXJdHk4sTw6I4TZ5d0khNh9tvrJQ4X/faY98h8
ebByHTh1+/bBc8SDESyrQ2DD4+jWCv2hKCYLrqmus2UPogBTAaB81qujEh76DyrO
H3SET8rzf/OkQonX0ne2Qi0CNsEmy2henXyYcQqNfi3t5F159dsST5sYjvwqp0t8
MvZCV7cIfwgXcqK6lqlC8wXo+VMROU+28W65Szzgg2gGnVqMU6Y9AVfPQB8bLQ6mU
rfdMZIZJ+AyDvWXpF9Sh01D49V1f3HZStz09jdvOmeFXklnN/biudE/F/Ha8g8VH
MGHOfMlm/xX5u/2RXscBqtNbn02gpXI61Brwv0YAWCv19Ij9WE5J280gtJ3kkQc2
azNs0A1FHQ98iLMcfFstjvzbzySPAQ/ClWxiNjrtVjLhdONMO/XwXV00jHRhs3jMh
LLUq/zzhS1AGBGNfISnCNLWhsQDGcgHKXrK1QzZ1p+r0ApQmwJG0wg9ZqRdQZ+c
fL2JSyIZrqr017Dves9lhcAAgIP/0zPniJshsHyJL56YffTm0Tm2016zXaGERmm
b6Ej2VhXQEjJUAov+HZ3odm2rVa0XR9F4RU7AFaIUedGmbET/Zp5uIT9CAuWODRq
wIaPdxXaS5HfEsDdwPC4rUigI3wU7unWq8zKgy8gx+I0XgPvkUmdwb+vcZ0Zr10
LC/SvyXyPNb87RANlttuDspFQ4/puUoxz/ICurJbBWx09oc29yyXiGX8YHf6NFA
UCSJH5W1fS9uIQEdip6dmFB7Q2qvOYHLF5nAg2zXvg8LzWI3dcxH0OXHV2KkG1E
bndUtq8cI8yz1+I6Pdfqb0DWvmIVVSHJMLtuZBUY1D8vso2ZK0//PcNMuqHU8ZfH
CAXwmrJAfzYhU8TP6P4YKqa/W4Cxy897yaaZHoR3iqhdDakMhrnDPa4isGJ20j
PEXpzQ5H4i7PEqk+phVxiEhbLzbdz1y0ZK/5dub5ci5mCwGZBVb9XTecZruwOe7
ptWlVbYhGBltUUFsF4wEwvoaxcC6EzFRpEqBRm+tgcgcfwULV9oywoMhLQwB9LD
VjnNkRoNuaEa2o8CnheehNU05NSASsSo4z2WWbkRGERZZaWiafLe+XhDC+hImWwO
dL5ZatkQ5qJp3GuFW0F1dqaYJLY1Knn9P+cpLhPEq5Hq27vcULDalL5AMnKIbusS
SrRP9MhWiQBMBBgRAGAMBQJBTKqFBQkCak+AAoJEIIdenepUv6CubCkAnl3adk2J
HcZLgEhuNLZPTye4iNgRAKctq+gBowVJ761YhVK2NMBi+8B3sw==
=j2zm
```

-----END PGP PUBLIC KEY BLOCK-----

Cryptography

RSA

Public Key: (e, n)

Private Key: (d, n)

To Encrypt

$$c = p^e \bmod n$$

To Decrypt

$$p = c^d \bmod n$$

Cryptography

RSA: Generating Keys

- 1) Choose 2 large primes, p and q .
- 2) Compute $n = p \times q$.
- 3) Choose e that's coprime to $[(p - 1) \times (q - 1)]$.
- 4) Compute d s.t. $(e \times d) \% [(p - 1) \times (q - 1)] = 1$.



Computer Science 50

Introduction to Computer Science I

Harvard College

Week 2

David J. Malan
malan@post.harvard.edu