

Harvard College

Week 2

David J. Malan  
malan@post.harvard.edu

## Or fher gb qevax lbhe binygvar!



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

0

1

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

2

## Bugs



see  
buggy{1,2}.c

Image from <http://www.history.navy.mil>.

3

## Casting

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

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

4

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

Image from <http://z.about.com/d/tvcomedies/17/n5/-/homersimpson.jpg>

5



## Functions

Scope, Local Variables, Temporary Variables

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

    tmp = a;
    a = b;
    b = tmp;
}
```

see  
buggy3.c

6

## Functions

Scope, Global Variables

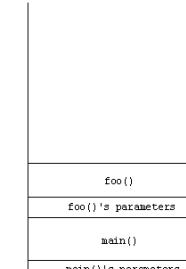
```
void
increment()
{
    x++;
}
```

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

7

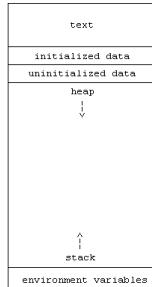
## The Stack

Frames



8

## Memory Management Sneak Preview



9

## Functions Return Values

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

see  
return{1,2}.c

10

## Arrays



See  
array.c, buggy6.c, string{1,2}.c, capitalize.c

Image from <http://computer.howstuffworks.com/c10.htm>.

11

## Free Resources

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

12

## Command-Line Arguments argc, argv

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

see  
argv{1,2}.c

13

## 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/>

14

## Cryptography

Or fher gb qevax lbhe binyvar!



Image from <http://www.radioarchives.org/annex/>.

15

## Cryptography Enigma Machine



Image from [http://en.wikipedia.org/wiki/Enigma\\_machine](http://en.wikipedia.org/wiki/Enigma_machine).

16

## Cryptography Secret (Symmetric) Keys

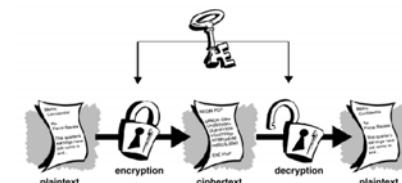


Figure from <http://www.nuitairi.de/crypto.html>.

17

## Cryptography

Caesar Cipher

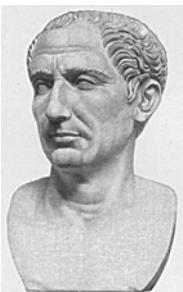


Image from <http://commons.wikimedia.org/wiki/Image:Her-Caesar.jpg>.

18

## Cryptography

Caesar Cipher

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

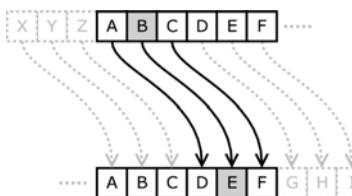


Image from [http://en.wikipedia.org/wiki/Caesar\\_cipher](http://en.wikipedia.org/wiki/Caesar_cipher).

19

## 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
	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓

20

## Cryptography

DES

72,057,594,037,927,936

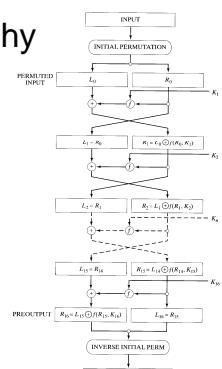


FIGURE 3-14 DES.

Figure from Larry Nyhoff's C++: An Introduction to Data Structures

21

## Cryptography

Public and Private (Asymmetric) Keys

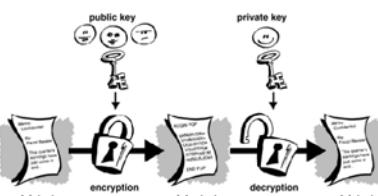


Figure from <http://www.nuitari.de/crypto.html>.

22

## Cryptography

PGP

```
-----BEGIN PGP PUBLIC KEY BLOCK-----  
Version: PGP Key Server 3.1.4  
  
mQINBQDwYX...  
-----END PGP PUBLIC KEY BLOCK-----  
  
-----BEGIN PGP PRIVATE KEY BLOCK-----  
Version: PGP Key Server 3.1.4  
  
uAj...  
-----END PGP PRIVATE KEY BLOCK-----
```

Ron Rivest's public key from <http://pgp.mit.edu/>.

23

## Cryptography

RSA

Public Key:  $(e, n)$   
Private Key:  $(d, n)$

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

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

Ron Rivest's public key from <http://pgp.mit.edu/>.

24

## 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.  $(e \times d) \% [(p-1) \times (q-1)] = 1$ .

Ron Rivest's public key from <http://pgp.mit.edu/>.

25

## Computer Science 50

Introduction to Computer Science I

Harvard College

Week 2

David J. Malan  
[malan@post.harvard.edu](mailto:malan@post.harvard.edu)

26