Encryption

CS2308
Fall2008
"Supplement"

Encryption

- encryption is the process of transforming information (referred to as plaintext) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. [Wikipedia]

Correctness

- We can use any function that maps one character to another, as long as it meets the following property:

For any characters a and b, f(a) != f(b)

- In other words, no two characters should map to the same character
- Should be a one to one mapping

Why xor

- xor is exclusive or:

```
0 ^ 0 = 0
0 ^ 1 = 1
1 ^ 0 = 1
1 ^ 1 = 0
```

- if you bitwise xor two characters together you get a character (no overflow)
- if you pick a given character as a key, and define f(a) = a ^ key, then f(a) is one to one.

More properties of xor

- (B ^ A) ^ A = B
- Example:

```
'a' ^ '2'
61hex 32hex
0110 0001
0011 0010
0101 0011
= 53hex = 'S'
```

```
'S' ^ '2'
53hex 32hex
0101 0011
0011 0010
0110 0001
= 61hex = 'a'
```

Simple xor cipher

- (B ^ A) ^ A = B
- a string of text can be encrypted by applying the bitwise XOR operator to every character using a given key. To decrypt the output, merely reapplying the key will remove the cipher.
- [password management does not require decryption]

More properties of xor

- If characters a and b both start with 0 (are less than 128) then a ^ b will start with 0 (be less than 128)

```
0xxx xxxx
0yyy  yyyy
=
0zzz  zzzz
```

- All characters will stay out of the "extended ascii" range
- May still have "unprintable" chars (0-31,127)