Blowfish Implementation Plan

Steven Grecu

|  |  |  |
| --- | --- | --- |
|  | Plain text instructions | Functions |
| 1 | “[Have] Alice create the secret shared key” | Alice.createKey() |
| 2 | “Alice will send the shared key to Bob through the UDP socket interface.” | Alice.sendKey() |
| 3 | Bob receives the key. | Bob.recvKey() |
| 4 | “Bob will reply with “OK” to complete the client-server interaction.” | Bob.sendKeyConfirm(Alice) |
| 5 | “Your program must first read this contract from an input file.” | Main.readContract() |
| 6 | Alice will “use your Blowfish encryption program and the shared key to encrypt the [...] contract[.]” | Alice.encrypt()  Blowfish.encrypt(contract, key) |
| 7 | “Alice will then send this encrypted document to Bob through the UDP socket interface.” | Alice.sendMsg(Bob) |
| 8 | “When Bob receives the encrypted message,” | Bob.recvMsg() |
| 9 | “he must use your Blowfish decryption algorithm and the shared key to decrypt Alice’s ciphertext.” | Bob.decrypt() Blowfish.decrypt(recvMsg, key) |
| 10 | “He will then sign the contract.” | Bob.sign() |
| 11 | “He will then encrypt the signed contract document using your Blowfish encryption program and the shared key.” | Bob.encrypt()  Blowfish.encrypt(sgnContract, key) |
| 12 | “Then he sends the encrypted document back to Alice through his UDP socket interface.” | Bob.sendMsg(Alice) |
| 13 | “Alice will receive Bob’s encrypted document through her UDP socket interface.” | Alice.recvMsg() |
| 14 | “She will then use your Blowfish decryption program and the shared key to decrypt Bob’s document into plaintext.” | Alice.decrypt() |
| 15 | “She verifies Bob’s signature and the sale is complete and legal.” | Alice.verifySig() |
| 16 | “Your program must write this plaintext final contract into an output file.” | Main.writeContract() |

# Blowfish algorithm implementation

(from Lecture 8 slides)

1. Use pi to initialize 18 P-arrays (each the length of the key) and 4 S-boxes (each the length of the key) containing 256 entries.
   1. calculate pi in hex, filling the above with each new digit calculated
2. XOR the P-arrays with key bits.
3. Encryption Loop:
   1. P first
   2. S second

All this is show except for the initialization with PI in the slides, with pseudocode copied from Wikipedia: <https://en.wikipedia.org/wiki/Blowfish_(cipher)#Blowfish_in_pseudocode>

# Classes

## Main

readContract()

writeContract()

## Alice

createKey()

sendKey()

encrypt()

sendMsg(Bob)

recvMsg()

decrypt()

verifySig()

## Bob

recvKey()

sendKeyConfirm(Alice)

recvMsg()

sendMsg(Alice)

encrypt()

decrypt()

sign()

## Blowfish

encrypt(String plaintext, String key)

decrypt(String ciphertext, String key)