CMPSCI 177 - Computer Security
Fall 2013
Third Homework - DES, Public Key, and Digital Rights Management

Due: Wednesday, 30 OCT 13 2:00pm

Part I: DES

1. Consider the following 64 bit key:
`1111000110011011011100011010001010100110101010111010001010011001`

What is the value of the key used for the fifth round of the DES encryption algorithm?

2. Consider the following 48 bit string:
`101110010110101110011011010001011011100101011100`

If this string is input to the s boxes in the DES encryption algorithm, what string is output from the s boxes?

Part II: Public Key

1. What is the totient of 46? Defend your answer.

2. Use the superincreasing sequence S=[3,7,13,27,51,102] modulus n=207, and multiplier w=19 to generate a public key sequence H for Merkle-Hellman.

3. Assume that you received the ciphertext C=364 from someone using the public key generated in exercise 2. You are to decipher C and determine the message M that was used to generate C.

4. Alice has chosen primes p=467 and q=479 and exponent e=70167 to use with the RSA algorithm. What does Alice publish as her public key?

5. Suppose Alice receives the following message from Bob, who used the public key from exercise 4 to encrypt it: 165369. Determine the plaintext that Alice obtains from this ciphertext.

Part III: Digital Rights Management

DRMBook Express

The release of the new DRMBook all-you-can-read streaming book services has turned the publishing business upside down! Users of the DRMBook client
https://github.com/cs177/DRMBook
are able to request and read any book that comes to their imagination, and the publishers of these books can rest easy with the knowledge that their Intellectual Property is protected by a world-class DRM system!

Or is it? Your job, as a member of Pirates, Inc, is to break the DRMBook copy protection, because culture should be free! The books, of course, originate in a markup language that is lost when they are rendered, so, similarly to video re-encoding, you can't just copy out the displayed text and call it good. You'll need to recover the original document. To prove that you can cut it as a pirate, you'll need to submit the original content of a book of your choosing. Good luck: the publishers jealously protect their stuff!