Digital Communications Coursework

1) AMXUWSWQJWXAATATCRAGMQIOU

2) THISISNOTHINGTODOWITHPIRATESATALL

3)
ASSOONASWESTARTEDPROGRAMMINGWEFOUNDTOOURSURPRISETHATITWASNTASEASYTOGETPROGRAMSRIGHTASWEHADTHOUGHTDEBUGGINGHADTOBEDISCOVEREDICANREMEMBERTHEEXACTINSTANTWHENIREALIZEDTHATALARGEPARTOFMYLIFEFROMTHENONWASGOINGTOBESPENTINFINDINGMISTAKESINMYOWNPROGRAMSMAURICEWILKESDISCOVERSDEBUGGING

4i) 17^2 = 11 mod 139
17^4 = 121 mod 139
17^8 = 46 mod 139
17^16 = 31 mod 139
17^32 = 127 mod 139
125

4ii) 2345^2 = 195245 mod 265189
2345^4 = 221653 mod 265189
2345^8 = 77513 mod 265189
2345^16 = 143185 mod 265189
2345^32 = 182635 mod 265189
2345^64 = 70805 mod 265189
2345^128 = 215169 mod 265189
2345^256 = 207374 mod 265189
2345^512 = 132069 mod 265189
2345^1024 = 209853 mod 265189
2345^2048 = 200702 mod 265189
2345^4096 = 144460 mod 265189
2345^8192 = 173623 mod 265189
2345^16384 = 116932 mod 265189
2345^32768 = 212973 mod 265189
32548

4iii) 4733459^1 = 4733459 mod 75968647
4733459^2 = 49107677 mod 75968647
4733459^4 = 16238929 mod 75968647
4733459^8 = 67757406 mod 75968647
4733459^16 = 25488171 mod 75968647
4733459^32 = 64480977 mod 75968647
4733459^64 = 57889554 mod 75968647
4733459^128 = 19358089 mod 75968647
4733459^256 = 50744319 mod 75968647
4733459^512 = 56497489 mod 75968647
4733459^1024 = 54825938 mod 75968647
4733459^2048 = 38930457 mod 75968647
4733459^4096 = 49024383 mod 75968647
4733459^8192 = 51007254 mod 75968647
4733459^16384 = 24313 mod 75968647

4733459^32768 = 59341440 mod 75968647
4733459^65536 = 51988154 mod 75968647
621879
5i) Cipher = Message^e mod n (in this case e=65537and n=76282747)
5ii) 39964485
6i) Message = Cipher^e mod n (in this case e=3497603 and n=9436709)
6ii) 1101011
7i) Firstly 'decrypt' message with your own private Key (337722^ 3497603 mod 9436709), encrypt both message and signature separately ((message and the signature) ^ 65537mod 76282747) and then send both to the receiver.
7ii) M=33191197
S=59821766
8i) Decrypt both the message and the signature separately ((message and the signature) ^ 3497603 mod 9436709) and then encrypt the signature with your private key ((Decrypted signature) ^ 65537mod 76282747). If the message and the 'encrypted' signature match, then the message is from the right person.
8ii)
Decrypted Message=7406060
Decrypted Signature=8180219
Decrypted Signature 'encrypted' with banks public key = 64026314
8iii) Decrypted Message and the Decrypted Signature encrypted with the banks public key are not equal and therefore it is not a valid message.
9) If you choose a random number < n and create message m =R^(public key of who you are pretending to be) mod n (i.e. R^53407 mod 122269479 send (M,S=R) encrypted with the recipients public key and modulus. They will decrypt it normally and the message with fit with the signature. Assuming the bank correctly decrypts the message for R=100 they will have an M=97612969 and S=100 which when decrypted (100^ 53407 mod 122269479).
10) Because the pin is only three digits long it is possible to just use brute force. Bob's new pin is 777. This is because I wrote a program that encrypted all the possible combinations for a three-digit pin and then if they appeared in the message they were outputted. The only output was 777.