Question 1

1 / 1 pts

What name do we use when referring to the originator of an encrypted message: Alice What name do we use when referring to the recipient of an encrypted message: Bob What name do we use when referring to the individual attempting to intercept an encrypted message: Eve

Answer 1:

Alice

Answer 2:

Bob

Answer 3:

Eve

Question 2

1 / 1 pts

Several symbols are used to describe the various components of an encrypted message exchange. Match the symbol with its description.

Encrypted text	Mc
Human-readable text	Mp
Symmetric encryption algorithm	C
Algorithm producing ciphertext from plaintext (but not the other way around)	C+
Algorithm producing plaintext from ciphertext (but not the other way around)	C-
The password used both to encrypt and decrypt a message	K
The password used to encrypt a message (but not decrypt it)	K+
The password used to decrypt a message (but not encrypt it)	K-
A unique token or value representing the message	D

Partial

Question 3

0.83 / 1 pts

XOR

C+(Mp, K) FOR i - each token i

C+(Mp, K) FOR i - each token in Mp Mc[i] - Mc[i] XOR K RETURN Mc

Codebook

C+(Mp, K) FOR i - each token i

C+(Mp, K) FOR i - each token in Mp Mc - K[Mp[i]] RETURN Mc

AES

Cipher(byte in[4*Nb], byte ou

Cipher(byte in[4*Nb], byte out[4*Nb], word w[Nb*(Nr+1)]) byte state[4,Nb] state - in AddRoundKey(state, w[0, Nb-1]) for round - 1 step 1 to Nr-1 SubB

Caesar

C+(Mp, K) FOR i - each token i

C+(Mp, K) FOR i - each token in Mp Mc[i] - (Mp[i] + K) % sizeAlphabet RETURN Mc

Book

C+(Mp, K) offsetPrevious - 0 F

C+(Mp, K) offsetPrevious - 0 FOR i - each token in Mp offsetNext - offsetPrevious + random() offsetNext - findWordBeginningWithLetter(offse

Polyalphabetic

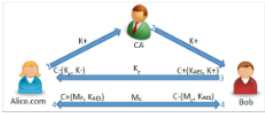
C+(Mp, K) FOR i - each token i

C+(Mp, K) FOR i - each token in Mp Mc[i] - (Mp[i] + K[i % sizeKey]) % sizeAlphabet RETURN Mc

Question 4

1 / 1 pts

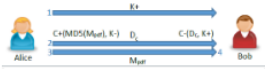
Match the application diagram with the application name.



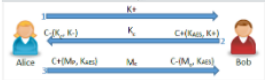
[Select]

[Select]

[Select]



[Select]



[Select]

Answer 1:

Certification

Answer 2:

Authorship

Certification. You selected this answer.

Answer 3:

Confidentiality

Answer 4:

Integrity

Answer 5:

KeyExchange

Question 5

10 / 10 pts

Decrypt the following message that was encrypted with +3 using the Caesar Cipher:

`PRURQLWHQIRXU`

Write the answer in ALLCAPS with no spaces.

MORONITENFOUR

Question 6

10 / 10 pts

Decrypt the following message that was encrypted with a book cipher where the key is "Proverbs 3."

```
50 216 55 23 9 27 10 96 72 59 216 101
```

Note that there are many possible ways to decipher this. The numbers could be absolute position from the front of the chapter, or they could be relative to each other. They could correspond to words, or they could correspond to letters. Headings, punctuation, and numbers may or may not be ignored. You will need to try many things.

Write the answer in ALLCAPS with no spaces.

TRUSTTHELORD

Question 7

5 / 5 pts

Using the Golden Bug, what is the key for the following Caesar Cipher message?

```
ESFQQWSJKSYGAUGFLJSULWVSFAFLAESUQOALZSEJOADDASE
DWYJSFVZWOSKGXSFSFUAWFLZMYMWFGLXSEADQSFVZSVGFUW
TWWFOWSDLZQTMLSKWJAWKGXEAKXGJLMFWKZSVJWVMUWVZAE
LGOSFLLGSNGAVLZWEGJLAXAUSLAGFUGFKWIMWFLMHGFZAKV
AKSKLWJKZWDWXLFWOGJDWSFKLZWUALQGXZAKXGJWXSLZWJK
SFVLGGCMHZAKJWKAVWFUWSLKMDDANSFKAKDSFVFWSJUZSJD
WKLGFKGMLZUSJGDAFSLZAKAKDSFVAKSNWJQKAFYMDSJGFWA
LUGFKAKLKGXDALLDWWDKWLZSFLZWKWSKSFVSFVAKSTGMLLZ
JWWEADWKDGFYALKTJWSVLZSLFGHGAFLWPUWWVKSIMSJLWJG
XSEADWALAKKWHSJSLWVXJGELZWESAFDSFVTQSKUSJUWDQHW
JUWHLATDWUJWWCGGRAFYALKOSQLZJGMYZSOADVWJFWKKGXJ
WWVKSFVKDAEWSXSNGJALWJWKGJLGXLZWESJKZZWFLZWNWYW
LSLAGFSKEAYZLTWKMHHGKWVAKKUSFLGJSLDWSKLVOSJXAKZ
FGLJWWKGXSFQESYFALMVWSJWLGTWKWWFWSJLZWOWKLWJFW
PLJWEALQOZWJWXGJLEGMDLJAWKLSFVKSFVOZWJWSJWKGEWE
AKWJSTDWXJSEWTMADVAFYKLWFSFLWVVMJAFYKMEEWJTQLZW
XMYALANWKXJGEUZSJDWKLGFVMKLSFVXWNWJESQTWXGMFVAF
VWWVLZWTJAKLDQHSDEWLLGTMLLZWOZGDWAKDSFVOALZLZWW
PUWHLAGFGXLZAKOWKLWJFHGAFLSFVSDAFWGXZSJVOZALWTW
SUZGFLZWKWSUGSKLAKUGNWJWVOALZSVWFKWMFVWJYJGOLZG
XLZWKOWWLEQJLDWKGEMUZHJARWVTQLZWZGJLAUMDLMJAKLK
GXWFYDSFVLZWKZJMTZWJWGXLWFSLLSAFKLZWZWAYZLGXXAX
LWWFGJLOWFLQXWWLSFVXGJEKSFSDEGKLAEHWFWLJSTDWUGH
HAUWTMJLZWFAFYLZWSAJOALZALKXJSYJSFUW
```

I wrote a program to help me crack this. Just a few lines of C++ code.

Write the key as a positive number.

18