Assignment 5

1.

a.

When all cards share the same key, it is possible to get a card and crack the security for all the other cards because they share that same key. When all cards have different keys, you have to break each of those keys individually.

b.

The card is identified because the card C has to decrypt a random nonce and send it back to the terminal. Terminal T does not have to identify itself.

c.

The terminal now has to prove that it is a terminal possessing the masterkey because the terminal needs to encrypt a random nonce send by the card C.

2.

a.

Plaintext:	011	111	101	001
Key:	101	101	101	101
XOR:	110	010	000	100
Substitution:	100	011	001	010

b.

Plaintext:	011	111	101	001
IV:	111	000	011	110
XOR:	100	111	110	111
Key:	101	101	101	101
XOR:	001	010	011	010
Substitution:	000	011	110	011

c.

With CBC mode, all characters of the ciphertext are calculated by the characters before that character in the ciphertext where as with ECB, all characters are only calculated with the key used.

d.

We need to get to Key = 111. For the key to be 111, the substitution of the characters before the key is the same as the key used after that substitution. Therefore, the substitution is also 111. When we substitude back to the plaintext, we get a XOR of: 101. The IV is 111 so when we XOR 111 with 101 we get 010. The plaintext we have to add before the original plaintext message is 010. This works because we will get 111 at the end of the encryption block, which we then use to encrypt the next block of the plaintext.

e.

?
f.

Ciphertext:	111	100	101
IV:	010	000	001
XOR:	101	100	100
Key:	100	100	100
XOR:	001	000	000
Substitution:	000	001	001

Ciphertext:	110	100	101
IV:	010	001	000
XOR:	100	101	101
Key:	100	100	100
XOR:	000	001	001
Substitution:	001	000	000

I: Three bits are changed.
II: Three blocks are different.
III: For every bit that changes, each bit on that same place in the next block changes.

3.

a.

Counter:	0	1	2
IV:	100	101	110
Key:	101	101	101
XOR:	001	000	011
Substitution:	000	001	110

b.

Plain:	001	110	111
Key:	000	001	110
XOR:	001	111	001
Substitution:	000	101	000

c.

Plaintext 1:	010	110	110
Ciphertext 1:	110	001	101
Substitution:	100	000	111
XOR:	110	110	001

This is also the keystream.

Ciphertext 2:	101	011	111
Substitution:	111	010	101

Now XOR with keystream:

Keystream:	110	110	001
XOR:	001	100	110 (plaintext)