Solutions 3

CSC 152 / 252 – Cryptography

Please notify me of any errors you find. If you need help, ask.

1) *The AES S-box is a permutation, and therefore could be used in the modes of operation we learned (ECB, CBC, CTR, OFB). Use the S-box in each of the modes to encrypt "abc". In modes that need padding use* 10^* *padding. For modes that need an IV use 01010011. For modes that need a nonce, use 0110. Note that the S-box would never be used this way, I'm just using it as a readily available permutation for practice.*

Will be done in class.

2) *Let's say that a ciphertext that was created using a mode-of-operation has a single bit toggled in it's i-th block before decryption. How damaging is it to the decryption? Describe the damage with respect to errors in the resulting plaintext blocks (eg, "plaintext block i has a single bit error", or "all plaintext blocks later than i look random", etc). Do this for each of the four modes ECB, CBC, CTR, OFB.*

ECB) The i-th plaintext block is scrambled. CBC) The i-th plaintext block is scrambled and the next plaintext block has a single bit error. CTR and OFB) The i-th plaintext block has a single bit error.

3) *You are given a black box f that has either a standard 52-card deck-of-cards or a 48-card deck-of-cards for the game pinochle. You are allowed to activate f once, upon which a card is chosen at random and you are given the card. In pseudocode, give an algorithm that uses f once and then guesses either "standard" or "pinochle". Evaluate the advantage your algorithm achieves.*

When choosing a random card, the card values 2–8 each have probability $1/13$ of being selected from a regular deck and probability 0 of being selected from a pinochle deck. The cards 9–A each have probability $1/13$ of being selected from a regular deck and probability $1/6$ of being selected from a pinochle deck. This means we can leverage the differences in probabilities to get some advantage: either guess "standard deck" when seeing 2–8, or guess "pinochle deck" when seeing 9–A (these are actually identical strategies but with complementary if-conditions). Here's a distinquishing algorithm.

```
x = f()
if (x is 9, 10, J, Q, K, or A)
   guess "pinochle"
else
   guess "standard"
```

The resulting advantage is $\Pr[\text{guesses pinochle} \mid \text{deck is pinochle}] - \Pr[\text{guesses pinochle} \mid \text{deck is standard}] = 1 - 6/13 = 7/13$.

4)