Problems in cryptology, week 5

Exercise 5.1 CBC mode (Cipher block chaining mode) of encryption for a block cipher follows the rule

$$c_i = E_K(c_{i-1} \oplus m_i), i = 1, 2, \ldots$$

where c_0 is some fixed and known initial value, $m_1, m_2, \ldots$ is the plaintext and $c_1, c_2, \ldots$ is the ciphertext. Explain how the receiver decrypts the ciphertext to obtain the plaintext.

Exercise 5.2 Another mode of operation is the *counter mode*. This mode will turn the block cipher into a stream cipher. The keystream sequence is given by

$$\mathbf{z} = E_K(0), E_K(1), E_K(2), \ldots.$$

Assume that the block cipher is DES (56 bit key and 64 bit block size). Explain how you can build a distinguisher that, with high probability, can tell you if a given sequence comes from DES in counter mode. The required length of $\mathbf{z}$ should be slightly larger than 2^{32} blocks.

Hint: Since E_K is a permutation we have $E_K(x) \neq E_K(y)$ if $x \neq y$.

Exercise 6.1 Consider the RSA cryptosystem with the public parameters $n = 4003997$ and $e = 379$. Assume you know that $\phi(n) = 3999996$.

a) Find the decryption exponent d.

b) Find p and q such that $n = pq$.

Exercise 6.2 The following system for key agreement was proposed for mobile radio in the US, but for obvious reasons it was never implemented. Alice and Bob wants to communicate using a conventional encryption system. To create a key for this system they use a key distribution center, KDC, which publishes $n = pq$ but keeps p and q secret. Alice randomly chooses a number $R_A,\ 0 < R_A < n$, and sends $R_A^3 \bmod n$ to the KDC. Bob randomly chooses a number $R_B,\ 0 < R_B < n$, and sends $R_B^3 \bmod n$ to the KDC. Since the KDC knows both p and q, it can find R_A and R_B. The KDC sends $R_A + R_B \bmod n$ to Alice who finds R_B by subtracting her known number R_A. R_B is now the key agreed by Alice and Bob.
An attacker, Eve, can find the key used by Alice and Bob by pretending that she wants to communicate with her friend Gus. Eve picks $R_C,\ 0 < R_C < n,\ gcd(R_C, n) = 1$. She then intercepts Alice's transmission of R_A^3 and sends $R_A^3 R_C^3 \bmod n$ to the KDC. Gus then picks the integer $R_D,\ 0 < R_D < n$ and sends $R_D^3 \bmod n$ to the KDC. At the same time he sends R_D to Eve. Eve will now receive $R_A R_C + R_D \bmod n$ from the KDC. Now Eve can find the value R_A and after intercepting $R_A + R_B$ that is sent from the KDC to Alice, Eve can find the key R_B agreed by Alice and Bob.

a) Assume that you are the KDC. Let $n = pq,\ p = 11,\ q = 17$ You receive the number 104 from Alice and 58 from Bob. Which value is sent back to Alice?

b) Use the result from a) and the fact that n is public. Assume that Eve picks the number $R_C = 160$ and Gus picks $R_D = 49$. The value sent to Eve from the KDC is 122. Find the key used by Alice and Bob.

Exercise 6.3 Show that RSA is not secure against a chosen ciphertext attack, i.e., if an attacker observes $c = m^e \bmod n$, show how he can find m by requesting a decryption of $c' \neq c$.

Hint: use the homomorphic property of RSA stating that

$$(m_1 m_2)^e \bmod n = (m_1^e \bmod n)(m_2^e \bmod n) \bmod n.$$

Exercise 6.4 Assume that we have an RSA crypto system with $p = 23$ and $q = 29$. The encryption exponent is chosen as $e = 3$.

a Determine the decryption exponent d.

b Decrypt the ciphertext $c = 2$.

c Decrypt the ciphertext $c = 2$ using the chinese remainder theorem.