CS294-3: Algorithms in the real world | Assignment 2 (Cryptography)

Due: Wednesday Oct 1, 1997

Problem 1:

Assume you design an encryption scheme with a single round DES (instead of the usual 16 rounds and ignoring the initial and final permutations). If you know a message cipher pair (m_1, c_1) for a key k for the values given below, what is m_2 assuming $c_2 = DES1_k(m_2)$. Assume the following hexidecimal values for m_1, c_1 and c_2.

$$\begin{aligned} m_1 &= \texttt{3F72D4E6 04CD825B} \\ c_1 &= \texttt{04CD825B 8E25E338} \\ c_2 &= \texttt{04CD825B 327C7D29} \end{aligned}$$

If you show the first 2 (leftmost) hexidecimal digits of m_2 that will convince me you know the rest.

Problem 2:

Assume we have a 3×3-bit s-box used in a block ciphers. For each of the following three substitutions explain what is wrong.

Input	out_1	out_2	out_3
0	2	0	4
1	5	4	3
2	3	1	7
3	7	5	2
4	0	2	5
5	4	6	0
6	3	3	6
7	1	7	1

Problem 3:

(a) Assuming p and q are primes, express $x^{-1} \bmod pq$ as a positive power of x.

(b) Given public key $e = 3$, $n = 391$ encode the value 45 using RSA.

(c) Assuming the same public key, decode the value 105 (you might want to write a short program to do it).

(d) In RSA for some n lets say $e = 3$ (a standard choice in some systems). If I accidentally give away d show how one can use this information to factor n.

Problem 4:

(a) Using ElGamal Encryption with the public key $p = 11, g = 7, y = 5$ encrypt the value 9 with random $k = 3$.

(b) Decrypt the pair (2,2).

(c) Given $p = 11$ why is 10 a bad value for g?

Problem 5:

(a) Generate the first 4 bits of the BBS random bit generator assuming that $n = 77, r_0 = 39$.

(b) For an arbitrary Blum integer $n = pq$ give an upper bound on the period of the generator (how many iterations it takes before it repeats). This need not be the strongest upper-bound but you will get more credit the stronger it is.