TOPIC: BREAKING DES TYPE SYSTEMS

1) BACKGROUND INFO

-From the beginning when the National Bureau of Standards released DES, there has been controversy surrounding the cryptographic algorithm.

--Many were concerned about possible IBM trapdoors and about the key size being too small.

2) 3 BASIC APPROACHES FOR ATTACKING DES

1) Differential Cryptanalysis

-Was introduced by Biham and Shamir around 1990, though it was probably known much earlier by the designers of DES (you will understand why later)

-The method is a chosen plaintext method and the idea is to compare the differences in different ciphertexts for chosen plaintexts and thus deduce information about the key.

-It basically gives us information about possible key arrangments.

-EXAMPLE

2) DISTRIBUTIVE COMPUTATION/BRUTE FORCE

-The distributive computation approach is probably the most popular attack method.

--Like we talked about it in class, when RSA issued a challenge to break DSA in 1997, it only took 5 months to submit the winning key and this was done by distributive computation.

--Rocke Verser had implemented a program where he used thousands of computers over the internet and he ended up spanning 25% of the keyspace before finding the key.

--The following year 85% of the keyspace was spanned by distributive computation in only 39 days.

3) MEET IN THE MIDDLE ATTACK

-A successful attack when dealing with double encrypted DES systems.

-Assume Eve has intercepted a message m and a double encrypted ciphertext $c = E_{K2} (E_{K1} (m))$. She wants to find k_1 and k_2. She first computes and stores $E_K(m)$ for all possible ks. She then computes $D_K(c)$ for all keys k. There has to be at least 1 match.

-These 2N computations are much less than the N^2 computations needed to brute force a double encrypted DES system.

TOPIC: BREAKING DES TYPE SYSTEMS

3) METHODS TO IMPROVE DES SECURITY

1) **Triple DES**: using DES 3 times. Roughly equivalent to a 112 bit key.

2) **Employ a new system that can take in a larger keysize than 56 bits.**

3) **Choose 3 keys and perform K_3 XOR E_{K2} (K_1 XOR m)**
-In other words, modify the plaintext by XORing with K_1 then apply DES with K_2 then XOR result with K_3. (Great way to diffuse and shown to be really secure)

TOPIC: BREAKING DES TYPE SYSTEMS

BREAKING DES-QUESTIONS/PROBLEMS

1. What type of attack method is best for the following:

   a) 5 Round DES system
   b) Regular 16 round DES system
   c) Double Encrypted DES system

2. Find the 4 possible keys using a 1-round DES system (like we have done in class) with 12-bit input (0011 1100 0011) and 12-bit output (1111 0100 0011)