Exercise 1: Show that DES has the property that \( \text{DES}_k(x) = \text{DES}_k(x) \) for every key \( k \) and input \( x \) (this is called the complementary property of DES). Show how this can be used to carry out a chosen-plaintext attack (with only two queries to a DES computation oracle computing \( O(x) = \text{DES}_K(x) \) where \( K \) is the key being searched for) to find the key \( k \) by locally running DES encryption only \( 2^{35} \) times (instead of \( 2^{65} \) times).

Exercise 2: Say the key schedule of DES is modified as follows: the left half of the master key is used to derive all the sub-keys in rounds 1–8, while the right half of the master key is used to derive all the sub-keys in rounds 9–16. Show an attack on this modified scheme that recovers the entire key in time roughly \( 2^{28} \).

Exercise 3: Consider using DES as a fixed-length collision-resistant hash function in the following way: Define \( h : \{0,1\}^{112} \to \{0,1\}^{64} \) as \( h(x_1\|x_2) \overset{\text{def}}{=} \text{DES}_{x_1}(\text{DES}_{x_2}(0^{64})) \) where \( |x_1| = |x_2| = 56 \).

1. Write down an explicit collision in \( h \).
2. Show how to find a pre-image of a given value \( y \) (that is, \( x_1, x_2 \) such that \( h(x_1\|x_2) = y \)) in roughly \( 2^{56} \) time.
3. Show a more clever pre-image attack that runs in roughly \( 2^{32} \) time and succeeds with high probability.

Exercise 4: Compute \( [101^{4,800,000,023} \mod 35] \) (by hand).

Exercise 5: The extended Euclidean algorithm eGCD receives input \( a, b \) and outputs \( d = \gcd(a, b) \) along with \( X, Y \in \mathbb{Z} \) such that \( Xa + Yb = d \). The algorithm works as follows:

- If \( b \) divides \( a \), then return \( (b, 0, 1) \)
- Else:
  1. Compute integers \( q, r \) with \( a = qb + r \) and \( 0 < r < b \)
  2. Set \( (d, X, Y) \leftarrow \text{eGCD}(b, r) \) // note that \( Xb + Yr = d \)
  3. Return \( (d, Y, X - Yq) \)

Prove that the output is correct and that the algorithm runs in polynomial time.