Problem 1 Data Encryption Standard (CIS 4362 and MAT 5932) 4+5=9 Points

The DES algorithm makes use of 16 round keys, that are derived from a 56-bit key $K$ by means of a key scheduling algorithm. The key scheduling algorithm is described in the appendix of the handout (FIPS PUB 46-3) you received in class.

a) Show that there are at least two possible choices for $K$, so that all round keys are identical.

b) What happens, if we encrypt a 64-bit block $M$ twice with DES under such a key $K$, i.e., if we compute $\text{DES}_K(\text{DES}_K(M))$ with all round keys being identical?

Problem 2 Finite Fields (CIS 4362 and MAT 5932) 4+4=8 Points

Consider the finite field $F := \mathbb{Z}_2[X]/(X^4 + X + 1)$

a) Find a primitive element of $F$, i.e., an element $\alpha \in F$ such that all non-zero elements in $F$ can be written as a power of $\alpha$.

b) Compute $X^{11} \in F$ with at most five multiplications (a squaring operation counts as a multiplication, too).

Problem 3 Diffie-Hellman (CIS 4362 and MAT 5932) 4+4=8 Points

a) Consider the additive group $G := (\mathbb{Z}_{12345678923}, +)$. Compute the discrete logarithm of $42 \in G$ w.r.t. to the base $4 \in G$.

b) Assume we execute the Diffie-Hellman Key Exchange in a cyclic group $(G, \cdot)$ of order $3 \cdot 7 \cdot 17 \cdot p$ where $p > 2^{2048}$ is prime. Eve eavesdrops the value $g^x$ sent by one of the two protocol participants and notices that $(g^x)^{3 \cdot 7 \cdot 17} = 1$, where 1 denotes the identity element in the group $G$. Explain how Eve can find the established secret key $g^{xy}$. You may assume that Eve knows a plaintext-ciphertext pair that has been computed with the key $H(g^{xy})$ for a known a cryptographic hash function $H$. 