Problem 1 Let \( p \) be a 128-bit prime and let \( \mathbb{Z}_p \) be the set of integers \( \{0, \ldots, p-1\} \). Consider the following encryption scheme. The secret key is a pair of integers \( a, b \in \mathbb{Z}_p \) where \( a \neq 0 \). An encryption of a message \( M \in \mathbb{Z}_p \) is defined as:

\[
E_{a,b}(M) = aM + b \mod p
\]

a) Show that when \( E \) is used to encrypt a single message \( M \in \mathbb{Z}_p \), the system is a perfect cipher. (For a definition, refer to notes from the first lecture.)

b) Show that when \( E \) is used to encrypt two messages \( M_1, M_2 \in \mathbb{Z}_p \), the system is not a perfect cipher.

Hint: Consider the case \( M_1 = M_2 \).

c) Show that a known plaintext attack with just two pairs of plaintext/ciphertext \( C_i = E_{a,b}(M_i) \) (\( i = 1, 2 \)) can recover the secret key \( a, b \) with high probability.

Problem 2 The following is a special case of a permutation cipher: Let \( m, n \) be positive integers. Partition the plaintext to segments of \( nm \) letters each. Write down each plaintext segment by rows in an \( n \)-by-\( m \) matrix. The ciphertext is created by going over the columns of the matrix. For example, if \( n = 3, m = 4 \) the plaintext ”cryptography” will lead to the matrix and the ciphertext will be ”ctaropyghpry”.

1
a. Decipher the ciphertext (generated in the abovementioned way, not necessarily with the same \( m \) and \( n \)) "myamraruiqtenctorahroywdsoyeourargdernogw".

b. Describe an effective method for deciphering long enough ciphertexts, encrypted by applying a regular substitution cipher first, followed by a permutation cipher as above. Limit your answer to no more than 8 lines.

**Problem 4** RTAU (an Internet Music Station) wishes to broadcast streamed music to its subscribers. Non-subscribers should not be able to listen in. When a person subscribes she is given a software player (which cannot be tempered with) with a number of secret keys embedded in it. RTAU encrypts the broadcast using a symmetric cryptosystem (private key) with a 128-bit key, \( K \). The secret keys in each legitimate player can be used to derive \( K \) and enable legitimate subscribers to tune in. When a subscriber cancels her subscription, RTAU will encrypt future broadcasts using a different key \( K' \). All legal subscribers should be able to derive \( K' \), while the canceled subscriber should not.

a. Suppose the total number of potential subscribers is less than \( n = 10^5 \). Let \( R_1, R_2, \ldots, R_n \) be \( n \) random independent values, 128 bits each. The player shipped to subscriber number \( u \) contains all the \( R_i \)’s except for \( R_u \) (i.e. each player contains 99999 keys). Let \( S \) be the set of currently subscribed users. Show that RTAU can construct a key \( K \), used to encrypt the broadcast, so that every subscriber in \( S \) can derive \( K \) (from the \( R_i \)’s in her player), while any single subscriber outside of \( S \) cannot derive \( K \). You may assume that the set \( S \) is known to everyone (e.g. it is a plain part of the broadcast). Briefly explain why your construction satisfies the required properties.

b. Is your construction in part (a) collusion resistant? That is, can two canceled subscribers combine the secrets embedded in their player to build a new operational player?

Remark: Much better solutions to this problem exist.

**Problem 5** In this problem we will become familiar with finite fields \( GF(p^k) \) where \( k > 1 \). Specifically, we will look at the field \( GF(2^4) \).
Find an irreducible polynomial $f(x)$ of degree 4 over the base field of characteristic 2, $\mathbb{Z}_2$. Implement the field $GF(2^4)$ in MAPLE using the two statements

\[
G16:=GF(2,4,f(x));
\]

\[
a := G16[\text{ConvertIn}](x);
\]

Once this is done, write a small loop which prints out all the primitive elements (multiplicative generators) in $GF(2^4)$. How many are there? The situation here is quite different than that of $GF(2^5)$. Briefly explain why. ($\text{ConvertOut}$ is a canonical representation of field elements, with higher degree monomials to the left.)

**Problem 6** Pick at random a 5 digit number $a$ and a 6 digit number $b$ that are relatively prime. Using just MAPLE’s \texttt{mod} command, run the Euclid \texttt{gcd} algorithm on your $a$ and $b$. How many \texttt{mod} steps did it take? Now run the extended \texttt{gcd} algorithm (again, employing just \texttt{mod} operations) and compute the multiplicative inverse of $a$ in $\mathbb{Z}_b$. Remark: Maple naturally has a built-in command for extended \texttt{gcd}, whose format is \texttt{igcd}($x,y,$’$a’,$’$b’). It returns the \texttt{gcd} of $x$ and $y$, and assigns $a$ and $b$ to the values satisfying $\text{gcd}(x,y) = ax + by$. You can use this to verify your \texttt{mod} computations.