Problem 1. (2+2+2 points)

(a) What is the size of the keyspace for the affine cipher over the English alphabet?

(b) Show that the composition of two affine ciphers is again an affine cipher.

(c) What do you think the largest problem is with the security of the Hill cipher?

Problem 2. (2+2 points)

(a) About how many times more time does a brute force key search take against a 112-bit DES than against a 56-bit DES?

(b) What is the Double version of the 56-bit DES, and why is it much less secure than a single 112-bit DES? (Enough to sketch your attack against Double DES, but not enough to give just the name of it.)

Problem 3. (3 points)

Find the linear recursion defining the sequence $0101110\,0101110\ldots$ of period 7.

Problem 4. (3 points)

What is the multiplicative inverse of x^{15} in $\mathbb{Z}_2[x] \pmod{x^4 + x + 1}$?

Problem 5. (3+3 points)

(a) Alice and Bob have the same modulus n for RSA, and encryption exponents e_A and e_B with $\gcd(e_A, e_B) = 1$. Charles sends them the same message m encrypted with these keys, resulting in the ciphertexts c_A and c_B. Eve intercepts both c_A and c_B. How can she find m?

(b) How do you achieve authentication and non-repudiation in RSA?

Problem 6. (3 points) Construct a hash function using the Cipher Block Chaining mode of operation of DES.

Problem 7. (4 points)

Test the primality of $n = 881$ with a Miller-Rabin test.

Problem 8. (5 points)

Factor $n = 2773$ using the elliptic curve $y^2 \equiv x^3 + 4x + 4 \pmod{n}$ and the point $P = (1, 3)$ on it. Here are the formulas for point addition on a curve $y^2 = x^3 + bx + c$: if $P_3 = P_1 + P_2$ and $P_i = (x_i, y_i)$ for $i = 1, 2, 3$, then

$$x_3 = m^2 - x_1 - x_2, \qquad y_3 = m(x_1 - x_3) - y_1,$$

where $m = (y_2 - y_1)/(x_2 - x_1)$ if $P_1 \neq P_2$, while $m = (3x_1^2 + b)/(2y_1)$ if $P_1 = P_2$.

Problem 9. (2+2+2 points)

(a) What is the difference between a key agreement and a key distribution protocol?

(b) Describe the Diffie-Hellman key agreement protocol.

(c) Describe the intruder-in-the-middle attack against Diffie-Hellman.