Problem 1(20pts): Determine all LFSR sequences generated by
(a) $x^3 + x + 1$
(b) $x^4 + x^3 + x^2 + x + 1$.

Problem 2(10pts): Show that $f(x) = x^6 + x + 1$ is irreducible and primitive over $GF(2)$. Constr finite field $GF(2^6)$ using f, and take α a primitive element in $GF(2^6)$. Using the shift-and-add discussed in class, find the sums: $\alpha^5 + \alpha^7$, $\alpha^5 + \alpha^8$ as powers of the primitive element.

Problem 3(10pts): Construct a Linear Feedback Shift Register of minimal length that produ output $(1001110)^\infty$.

Problem 4(20pts): Find all irreducible and primitive polynomials of degree 6 over $GF(2)$.

Problem 5(10pts): Suppose that m users want to be able to communicate with one another classical cryptosystem. Each user insists on being able to communicate with each other user withc remaining $m-2$ users eavesdropping. How many keys $K = (K_E, K_D)$ must be developed? How mar are needed if they are using a public key cryptosystem. Estimate both counts (and compare) if $m =$

Problem 6(20pts): An instance of the Hill cipher is defined as follows. The message blocks m ar $GF(2^3)^2$, which is generated by the polynomial $f(x) = x^3 + x + 1$ with root α. The keys $\mathcal{K}$ are ta be $\mathcal{K} = \{\text{all } 2 \times 2 \text{ invertible matrices over } GF(2^3)\}$. The encryption function is $e_K(m) = mK$.
(a) Encrypt the plaintext $m = (\alpha, \alpha^2)$ using the key $K = \begin{pmatrix} \alpha^2 & \alpha+1 \\ \alpha^2+1 & 1 \end{pmatrix}$.
(b) Explain why $\mathcal{K}$ cannot contain all 2×2 matrices.
(*For extracredit*: How many keys are there?)

Problem 7(20pts): In an RSA-system the public encryption function is $C = M^e \pmod n$ and the decryption function is $M = C^d \pmod n$, where $n = pq$ (p, q primes), M is the plaintext and C ciphertext. The public parameters are (n, e), and the secret parameters are (p, q, d).
(a) Can a user of RSA choose the encryption exponent e to be even, e.g. e = 1004?
(b)It is popular to choose $e = 3$ if possible, since a small e gives a fast encryption. Although, is considered to be a secure public-key system, errors are quite often made when implementing it instance, assume that $M \in \mathbb{Z}_{2^{64}}$ is encrypted using a 512-bit RSA number n and the corresponding Explain why this is completely insecure. As an example, find the plaintext corresponding to the ciph $C = 4921675101$ when $n = 349688448443 41$ and $e = 3$.

Problem 8 (20pts): Read the article "New Directions in Cryptography" by Diffie and Hellman answer the following problems/questions.

(a). The paper gives rationales for building encryption schemes that are secure against known plai attacks and chosen plaintext attacks, by discussing how such schemes remove restrictions tha placed on the ways of using them. Discuss these rationale in your own words.

(b). List all the limitations and shortcoming discussed in the paper about symmetric encryption sch

(c). Why is the Hill cipher not a very good choice for a public key cryptosystem?

(d). Enumerate some of the one-way functions they mention in their seminal paper.

Problem 9 (10pts): Use Pohlig-Hellman algorithm to compute the discrete logarithm $x = L_\alpha(\beta)$. $p = 101$, $\alpha = 2$. $\beta = 3$ (and so, $\beta \equiv \alpha^x \pmod p$)).