Answer the following questions explaining each step in each part.

---

1. (a) Search and define *knight tour*.
   (b) We use Spartan transposition with entry path a knight tour and then the chess board is read by rows, starting by the top row. Give a key $k = (d, f)$, according to the notation of Module 1.
   (c) How many keys are there that correspond to a closed knight tour? You can search this information on the web.
   (d) Choose a text and encrypt it using this cipher.
   (e) Can you decode the message

   EMODEUDRSRREOEUQALCSAAOOOALSSTLNTAOBVOAHBORINYENTLITUVABTAANBAEZ

   (without blank spaces), that corresponds to the next knight tour?

1	30	47	52	5	28	43	54
48	51	2	29	44	53	6	27
31	46	49	4	25	8	55	42
50	3	32	45	56	41	26	7
33	62	15	20	9	24	39	58
16	19	34	61	40	57	10	23
63	14	17	36	21	12	59	38
18	35	64	13	60	37	22	11

   (f) Give a procedure to check whether a given f corresponds to a knight tour.

2. (a) How must be a matrix K in order to be used for a Hill cipher?
   (b) A Hill cipher is used and an attacker knows the parameters $d = 7$ and $n = 26$. If the attacker can make an attack with chosen plain text of 50 characters, what text would give the key with less computation? Explain how you would obtain the key.

3. We are trying to determine one person among the list {Juan, Jaime, Jose, Antonio, Pedro, Julio, Ana, Maité, Carmen, Angeles, Mercedes, María}.

   (a) How many bits of information give the next fields? Which field gives more information and which field gives less information?
      - Gender
      - First letter
      - Number of letters in the name
      - Language of the name

   (b) Compute the conditioned entropy
      - $H(gender \mid firstletter)$
      - $H(firstletter \mid gender)$

   (c) If we denote
      - X = gender,
      - Y = first letter,

   check that $H(X) + H(Y \mid X) = H(Y) + H(X \mid Y)$.

4. (a) What is the largest period that a cipher sequence generated by a LFSR register with connection polynomial of degree 4 can have?
   (b) Give three polynomials f, g, h of $Z_2[x]$ of degree 4, such that
      - f is reducible,
      - g is irreducible but not primitive,
      - h is primitive.

   (c) Generate two different cipher sequences for the LFSR registers with

connection polynomial f, g, h, respectively.

(d) Check that the cipher sequences generated by f depend on the initial state.

(e) Check that the cipher sequences generated by f have period smaller than the maximum stated as an answer to the first question.

(f) Check that the cipher sequences generated by g all have the same period.

(g) Check that the cipher sequences generated by g have a period that is a divisor of the maximum stated as an answer to the first question.

(h) Check that the cipher sequences generated by h have period equal to the maximum stated as an answer to the first question.

(i) Check that different cipher sequences generated by h are just a cyclic permutation of each other.