1. (a) Let $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \in M_2(\mathbb{Z})$. Show that the associated linear map $L_A : \mathbb{Z}^2 \rightarrow \mathbb{Z}^2$ is injective (one-to-one). Moreover, show that $L_A$ is not surjective (onto) by finding an explicit vector which is not in the image of $L_A$ (and verify that it isn’t).

(b)* Let $R$ be a commutative ring and let $A \in M_n(R)$ an $n \times n$ matrix with coefficients in $R$. Using results from class, prove that if the associated linear map $L_A : R^n \rightarrow R^n$ is surjective, then $A$ is invertible. Conclude from this that $L_A$ is an isomorphism if and only if it is surjective.

(c)* If $A \in M_n(\mathbb{Z})$, give necessary and sufficient conditions in terms of $\text{det}(A)$ for $L_A$ to be injective, respectively, to be surjective.

2. (a) Make (by hand) a power and log table for $\mathbb{F}_17^\times$, using the generator 3. Use it to find the discrete logs $DL_3(5)$ and $DL_3(11)$, and to compute $1/5$ and $5/11$.

(b) Make (by hand) a power and log table for $\mathbb{F}_9 \simeq A_f$, where $f(x) = x^2 + 1 \in \mathbb{F}_3[x]$, using the generator $g := x + 1$. Use it to find the discrete logs $DL_g(2 + x)$ and $DL_g(1 + 2x)$, and to compute $(2 + x)(1 + x)$, $(2 + x)^4$ and $1/(1 + 2x)$.

3. **MAPLE problem (refer to the MAPLE instruction sheet):**

(a) Write a program `encode(m, n, e)` which uses the RSA method with public key $(n, e)$ to encode a given message $m$. (Here, $m$ is an integer with $0 < m < n$.)

(b) Use your program in (a) to write a program `encodelist(ml, n, e)`, which takes a message list $ml := [m_1, m_2, \ldots, m_r]$, and returns the encoded list $Ml = [M_1, M_2, \ldots, M_r]$, where $M_i = encode(m_i, n, e)$.

(c) Recall from class that the message *this is top secret* was translated in the number sequence [20080919, 00091900, 20151600, 19050318, 05200000]. Use your program in (b) to encode this message (or number sequence) with the public key $n = 2363612653$ and $e = 123456023$.

(d) Using the MAPLE command `ifactors(n)`, write a short program `crack(n, e)` which determines the secret code $d$ needed for decoding the messages encoded in (a).

(e) Using your programs, find $d$ for the example of (b), and use this to decode the message encoded above. (Check that you obtain the original message again!)

(f) Using your programs, decode (and interpret) the following secret message which Bob sent to Alice, whose public key is $(n_A, e_A) = (31396132518131, 1234567891211)$: $\text{Msg} := [16819316935214, 17923423920580, 31275178804025, 6211715922581]$. 
