

## **Project 2- Shift-Affine ciphers**

Write a mobile application that simulates two classical encryptions (shift, affine).

- For each encryption, the application has four functions: setup the encryption key, encryption, decryption, cryptanalysis.
- Setup the encryption key: allow a user to generate the key either randomly, or manually (entered by the user).
- The default space for plaintext/ciphertext/key is the set of small alphabet 'a' .. 'z', but the application allows the user to extend it to include: capital letter, digit 0..9, or some special characters such as space, \$, %, #, @.
- For more details about the encryption, decryption, and cryptanalysis see the lecture notes and textbook “Cryptography: Theory and Practice by Douglas Stinson”.

N.B. The maximum number of students in a group's project is 5.