1) Cryptotext "qbylycmnbyeys" was created using CAESAR-type cipher. Find the plaintext.

2) The AFFINE cipher is a special type of substitution cipher. We first encode letters of English alphabet by numbers:

A is 0, B is 1, C is 2,...,Y is 24, Z is 25.

Now we have $P = C = \mathbb{Z}_{26}$. The keys are of the form $k = (\alpha, \beta)$, where $\gcd(\alpha, 26) = 1$ (i.e. $\alpha$ and 26 do not have common factors). The encryption is defined by

$$E_k(x) = \alpha x + \beta \mod 26.$$  

When using the AFFINE cipher the cryptotext is "ipvalx". You also happen to know that the plaintext begins with "AR". Find out the whole plaintext.

3) (a) Is the encryption more secure if we apply AFFINE cipher twice with different keys but with the same modulus? Justify your answer.

(b) From implementation point of view it is useful if encryption and decryption operations are identical to each other. Find all keys in the AFFINE cipher such that the encryption and the decryption functions are identical.

4) You have found a piece of paper that reads "bpubh ai bhcpc epc rk hkpici ar cbkr". You also happen to know that the text was created by a substitution cipher. Find out the whole plaintext.

5) Prove the formulas

$$(a \mod n) + (b \mod n) \mod n = (a + b) \mod n,$$

$$(a \mod n)(b \mod n) \mod n = (ab) \mod n.$$  

6) Compute

$$987654319^{29} \mod 987654321.$$