

Q12) DTU/2K16/ MC/13

Assume a one time pad version of the Vigenère cipher. In this scheme, the key is a stream of random numbers between 0 to 26. For example, if the key is 3, 19, 5 then the first letter of plaintext is encrypted with a shift of 3 letters, the second with a shift of 19 letters, the third with a shift of 5 letters, and so on. Encrypt the plaintext "SENDMOREMONEY" with the key stream

9, 0, 1, 7, 23, 15, 21, 14, 11, 11, 2, 8, 9

P: S E N D M O R E M O N E Y

P_i : 18 4 13 3 12 14 17 4 12 14 13 4 24

K_i : 9 0 1 7 23 15 21 14 11 11 2 8 9

$C_i = (P_i + K_i) \cdot 26$ 4 14 10 9 3 12 18 23 25 15 12 7

C: B E O K J D M S X Z P M H

Hence, the final ciphertext is:

BEOKJDM SXZPMH