Homework 1
VE475 Introduction to Cryptography

Jiang, Sifan
jasperrice@sjtu.edu.cn
515370910040

May 17, 2019

Ex. 1 - Simple questions

1. Since Alice uses Caesar cipher and we already known the ciphertext, we can apply CCA to decrypt the ciphertext, "EVIRE". So, the 25 possible names of the place are: DUHQD, CTGPC, BSFOB, ARENA, ZQDMZ, YPCLY, XOBKX, WNAJW, VMZIV, ULYHU, TKXGT, SJWFS, RIVER, QHUDQ, PGTCP, OFSBO, NERAN, MDQZM, LCPYL, KBOXK, JANWJ, IZMVI, HYLUH, GXKTG, or FWJSF. However, only "ARENA" and "RIVER" are meaningful, which could be the meeting place.
2.
3.

Ex. 2 -