SPCS CRYPTOGRAPHY
HOMEWORK 12 (REALLY OPTIONAL)

Spend time on your project first - think about these problems only if you are bored, perhaps. You are strongly encouraged to work in groups, but you have to write up the solution on your own.

1. Bob also doesn't trust Eve. For some reason he has to flip a coin with Eve over phone. However, he does not know zero-knowledge proof. Can you help him design a fair coin-flipping protocol? Hint: Let $n = pq$ be product of two large distinct primes. For any squares mod n, there are 4 square roots mod n.

2. We did a lot of secret sharing these two days - yet if say, Carol is mallicious, she may not use the actual given secret in the reconstruction-of-secret step. How can Zelda make sure that this does not happen? Hint: commitment schemes.

3. Err.. you probably know what to do?

```
CICNH ITVYA EMFFG CZHJZ QLASP PMJGS GURDI FGJCC
MHQDM GKCYU MNHIT VYAEM NZITM CYFPZ HBRIM QESOJ
CILCO LAWHV YVJAA OJRGP FXWJR YHYKE EVEOF KMHXS
AFSWT JGWSC VFCTI XGUEF BTLVQ GCIAO VPMJX BLFWT
WHJZQ REOUJ DTXZH ICTMC EFLIT QVDCX YMQLF POSSL
CHMWQ EQPUC WKAGR DVFEG TDJPM GFOVY GCZSP VPPEO
PULDP MQLQW HINUE DUOEB RDRCW INGXG GERPM WQEWT
                    LFGRJ AR
```