VE475 Introduction to Cryptography
Homework 9

Jiang, Sifan
jasperrice@sjtu.edu.cn
515370910040

July 26, 2019

Ex. 1 - *Missile or not missile ...*

(t, w)-threshold scheme could be used, where $t = 10$ and $w = 30$. The general is given 10 shares. Each colonel is given 5 shares. Each clerk is given 2 shares.

Ex. 2 - *Asmuth-Bloom Threshold Secret Sharing Scheme*

Let $k \in \mathbb{Z}$ and $2 \leq k \leq n$.

Ex. 3 - *Shamir's Threshold Secret Sharing Scheme*

Ex. 4 - *Simple questions*

1.

Ex. 5 - *Reed Solomon codes*

1.

2.