Algorithms of Information Security

Exercises for *Cryptographic Protocols II* and *Malware*

Cryptographic Protocols II:

1. There are four people in the room and we know that exactly one of them is a spy. The other three people share secrets using Shamir's (3,2) scheme over $\mathbb{Z}_{11}$. The spy randomly chose his share. The four pairs are $P_1 = (1, 7), P_2 = (3, 0), P_3 = (5, 10)$ and $P_4 = (7, 9)$. Find out which pair was created by a spy.

   [Result: A spy is a person with a share of P_1.]

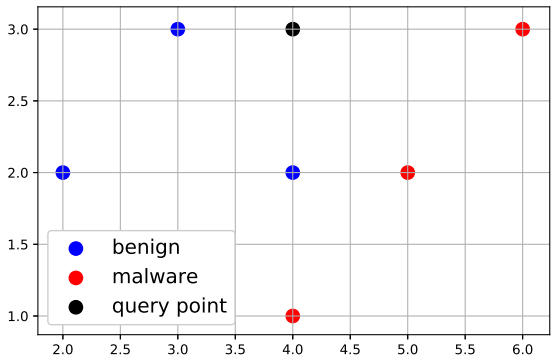
2. Alice and Bob used Shamir's no key protocol for the prime number $p = 31$. Alice chose a random number $a = 13$, while Bob chose $b = 11$. Alice's message $K^a \mod p$ was 8. What three messages did they send and what secret do they share?

   [Results: $A \to B : 8, A \leftarrow B : 8, A \to B : 2$ and the secret is $K = 2$.]

Malware II:

1. Let $T = \{((2, 2), \mathcal{C}), ((3, 3), \mathcal{C}), ((4, 2), \mathcal{C}), ((4, 1), \mathcal{M}), ((5, 2), \mathcal{M}), ((6, 3), \mathcal{M})\}$ be a training set, where $\mathcal{C}$ denotes the class of benign (clean) samples and $\mathcal{M}$ denotes the class of malicious samples. Let $x = (4, 3)$ be testing feature vector and the parameter $k = 3$ be number of nearest neighbors. Use k-Nearest Neighbor classifier and determine the class c for x.

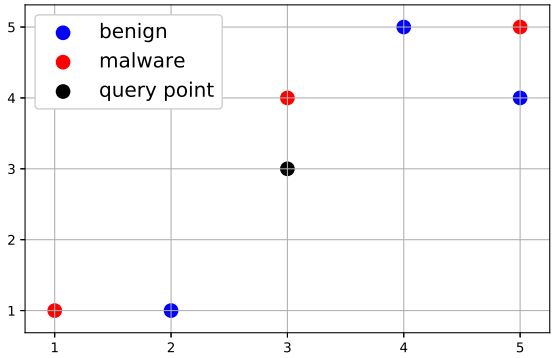
   Hint:



   [Result: The class of x is $c = \mathcal{C}$.]

2. Let $T = \{((2, 1), \mathcal{C}), ((4, 5), \mathcal{C}), ((5, 4), \mathcal{C}), ((1, 1), \mathcal{M}), ((3, 4), \mathcal{M}), ((5, 5), \mathcal{M})\}$ be a training set, where $\mathcal{C}$ denotes the class of benign (clean) samples and $\mathcal{M}$ denotes the class of malicious samples. Let $x = (3, 3)$ be testing feature vector and the parameter $k = 3$ be number of nearest neighbors. Use Distance Weighted k-Nearest Neighbor classifier and determine the class c for x.

   Hint:



[Result: The class of x is $c = \mathcal{M}$.]

3. Let $T = \{((a, a, b), \mathcal{C}), ((a, b, a), \mathcal{C}), ((b, a, a), \mathcal{C}), ((a, b, b), \mathcal{M}), ((b, a, b), \mathcal{M}), ((b, b, a), \mathcal{M})\}$ be a training set, where $\mathcal{C}$ denotes the class of benign (clean) samples and $\mathcal{M}$ denotes the class of malicious samples. Let $x = (b, b, b)$ be testing feature vector. Use Naive Bayes classifier and determine the class c for x.

   [Result: x is classified as malware, i.e. $c = \mathcal{M}$.]