NIE-AIB — Homework 5 – 24.11.2022

Instructions.

Complete the exercises and write your solutions on papers. Comment your solutions sufficiently. **A result alone without the solution is insufficient**. Submit your solutions to the MS Teams assignment "NIE-AIB, Homework 5" no later than December 7.

1 Exercise 1.

WKNN.

- Let $T = \{((2,2), \mathcal{C}), ((2,3), \mathcal{C}), ((3,3), \mathcal{C}), ((0,0), \mathcal{M}), ((0,1), \mathcal{M}), ((2,0), \mathcal{M})\}$ be a training set, where $\mathcal{C}$ denotes the class of benign (clean) samples and $\mathcal{M}$ denotes the class of malicious samples.
- Let $x_q = (2,1)$ be testing feature vector and the parameter $k = 3$ be number of nearest neighbors.
- Use Distance Weighted k-Nearest Neighbor classifier and determine c_q.

2 Exercise 2.

Naive Bayes.

- 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 $x_q = (a,a,a)$ be testing feature vector.
- Use Naive Bayes classifier and determine c_q.

3 Exercise 3.

Consider the following signature scheme. Alice chooses two large secret primes p, q and computes their product n. She also chooses an element $g \in \{0, \ldots, n-1\}$ such that g generates a subgroup of order r in $\mathbb{Z}_n^*$, where r is a large prime.
Alice's public key is a pair (n, g), and her private key is a number r.
To sign a message m, Alice finds x such that $xm = 1(\mod r)$. Then she computes the signature $s = g^x(\mod n)$. Suppose Bob has received a pair (m, s) from Alice.

- a. How is Bob able to verify her signature?
- b. Show that if r is a factor of exactly one of numbers $p-1, q-1$, then one can factor n using only a public key.

4 Exercise 4.

Alice and Bob use Shamir's no-key protocol to exchange a secret message. They agree to use the prime $p = 31883$ for their communication. Alice chooses the random number $a = 8647$ while Bob chooses $b = 10931$. It is known that Bob receives the first exchanged message $c_1 = K^a \mod p = 26843$. Calculate the remaining values c_2, c_3, and find the key K for Bob. Use the Extended Euclidean Algorithm to compute $a^{-1} \mod p-1$.