Quiz. 6

(Deadline April 18, 2024)

Problem 1

The Walsh-Hadamard Transform (WHT) is a series of procedures that effectively calculates the Hadamard transform of a one-dimensional signal with real values.

To aid in comprehension, we present the pseudocode below for a simple implementation of the Discrete Walsh-Hadamard Transform.

Walsh-Hadamard Transform:

```
def WHT(x):
    # Function computes (slow) Discrete Walsh-Hadamard Transform
    # for any 1D real-valued signal
    # (c) 2015 QuantAtRisk.com, by Pawel Lachowicz
    x = np.array(x)
    if (len(x.shape) < 2):  # make sure x is 1D array
        if (len(x) > 3):  # accept x of min length of 4 elements (M=2)
            # check length of signal, adjust to 2**m
            n = len(x)
            M = math.trunc(math.log(n, 2))
            x = x[0:2 ** M]
            h2 = np.array([[1, 1], [1, -1]])
            for i in range(M - 1):
                if (i == 0):
                    H = np.kron(h2, h2)
                else:
                    H = np.kron(H, h2)

            return (np.dot(H, x) / 2. ** M, x, M)
```

a) Please showcase the **recursive process** of the Walsh-Hadamard Transform using the pseudocode provided above.

b) Examine different **applications** of the Walsh-Hadamard Transform, highlighting how its properties offer advantages in each specific application.

Problem 2

The Miller-Rabin test is an algorithm based on probability that is employed to ascertain the primality of a given number. It operates by selecting random bases multiple times and examining if these bases offer substantial indications that the number is not prime.

The procedure consists of the following steps:

1. Given a number n, find an integer s and an odd number q such that $n - 1 = 2^s q$.
2. Choose a random number a from the range $[1, n - 1]$.
3. Compute $a^q \mod n$. If the result is 1 or $n - 1$, then n passes.
4. For i from 0 to $s - 1$, compute $a^{2^i q} \mod n$. If one of these is $n - 1$, n is again passes.
5. If none of the above conditions are met, n is composite.

It is typical to carry out trial divisions by small primes before conducting the Miller-Rabin test in order to promptly identify obvious composites.

a) What **happens** when we apply the Miller-Rabin test to numbers in the format pq, where p and q are large prime numbers?

b) Can we **break** RSA with it?

What to turn in:

a) The file you need to upload is structured as follows:

- <student_id>.zip
  - <student_id>.pdf

b) The <student_id>.pdf file should contain the solution to the provided problems.