Quiz 6

1.

a. to calculate the WHT recursively, we can first set

$$W_1 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

And let the input vector v has $N = 2^M$ elements, we can recursively calculate W_M by

$$W_{k+1} = \begin{bmatrix} W_k & W_k \\ W_k & -W_k \end{bmatrix} = W_k \otimes W_1$$

then calculate

$$r = \frac{1}{2^M}(W_m \cdot v)$$

as the result of WHT.

b. Walsh-Hadamard Transform can be used in Signal Processing, Data Compression, and Pattern Recognition.

Signal Processing:
WHT has the ability to efficiently represent signals with sparse frequency content. Additionally, the WHT has a fast implementation through algorithms like the Fast Walsh-Hadamard Transform (FWHT), making it suitable for real-time applications.

Data compression:
WHT efficiently represents signals with a few dominant coefficients, making it suitable for lossless and lossy compression. Its recursive nature allows for hierarchical compression schemes, where different levels of detail can be retained.

Pattern Recognition:
WHT can represent signals in a compact form makes it suitable for feature extraction. Moreover, its computational efficiency enables fast processing of large datasets, making it practical for real-world applications.

2.

a. when we conduct Miller-Rabin to $n = pq$, where p and q are large primes, we can find a witness to prove n is composite if conducted enough tests.

b. as for RSA, we **can't** break RSA with Miller-Rabin.

Since RSA encryption relies on the difficulty of factoring large composite numbers into their prime factors. While the Miller-Rabin test can help identify composite numbers efficiently, it doesn't directly aid in factoring them. So, even when we know a number is composite, to factorize it is still a hard job.