For the purposes of this module you should take the following as the definitions of a stream cipher, Vigenère cipher, and one-time-pad cipher.

A *stream cipher* over an alphabet A consists of a keyword $k = k_1k_2...k_n$ which is a sequence of elements of A of the same length as the plaintext $p = p_1p_2...p_n$, and a substitution table S which is an $|A| \times |A|$ array with entries from A with the property that no element of A appears twice in the same column of S. The rows and columns of S are labeled by the elements of A. The ciphertext $z = z_1z_2...z_n$ is given by $z_i = p_i \oplus k_i$ for $i = 1, 2..., n$, where $p_i \oplus k_i$ is the entry in row p_i and column k_i of S.

A *Vigenère cipher* is a stream cipher over the alphabet $\{a, b, c \ldots, z\}$ in which the substitution table is the Vigenère square.

A *one-time-pad cipher* is a stream cipher in which the keyword is a uniformly distributed random sequence of letters from A, and the substitution table is a Latin square.