ABSTRACT. A coding analogue of NTRU is derived. Its security is based on the difficulty of classical coding problems (computing the minimum weight, decoding an arbitrary syndrome) for the special class of pure double circulant $q$-ary codes. An attack on the public key is based on the special instance of a NP-complete problem: Minimum Distance over $GF(2^m)$. An attack on a ciphertext is based on the difficulty of Linear Decoding With Preprocessing a problem conjecturally not in $P$. Lattice attacks (LLL) are avoided. The speed of encryption/decryption of CTRU is the same as NTRU for the same value of $N$. A very secure system is achieved for $N = 256$. 