Cryptanalysis

Breaking the cipher

The Kerckhoffs' principle (1883)

"The enemy knows the system" - the security of a communication should not rely on the fact that the algorithms are secrets

➡ A cryptosystem should be secure even if everything about the system, except the key, is public knowledge

No security by obscurity