MODERN CRYPTOGRAPHY

1. THE OPPONENT KNOWS THE SYSTEM BEING USED

2. THE OPPONENT HAS ACCESS TO ANY AMOUNT OF CORREPONDING PLAINTEXT->CIPHERTEXT

3. THE OPPONENT MAY HAVE ACCESS TO THE KEY USED IN THE ENCRYPTING TRANSFORMATION. $E_k(M)=C$

4. SECURITY IS TO BE ACHIEVED BY THE OPPONENT NOT BEING ABLE TO CONSTRUCT THE DECRYPTING TRANSFORMATION $D_k(C)= M$

TRAPDOOR CIPHERS

A map c=E(m) from the message space M to the cipherspace C is said to be a trapdoor function if the construction of the the inverse map m=D[c] is of such theoretical complexity as to make it inaccessible to our present day computational tools.

NOTE:
A TRAPDOOR FUNCTION MAY BE SO TODAY....
BUT MAY NOT BE SO TOMORROW!!!!

TRAPDOOR CIPHERS

A map c=E(m) from the message space M to the cipherspace C is said to be a trapdoor function if the construction of the the inverse map m=D[c] is of such theoretical complexity as to make it inaccessible to our present day computational tools.

NOTE:
A TRAPDOOR FUNCTION MAY BE SO TODAY....
BUT MAY NOT BE SO TOMORROW!!!!