













After realizing the power of one-way functions, it is evident that their existence in cryptosystems is essential.

However, can a system be completely secure?

