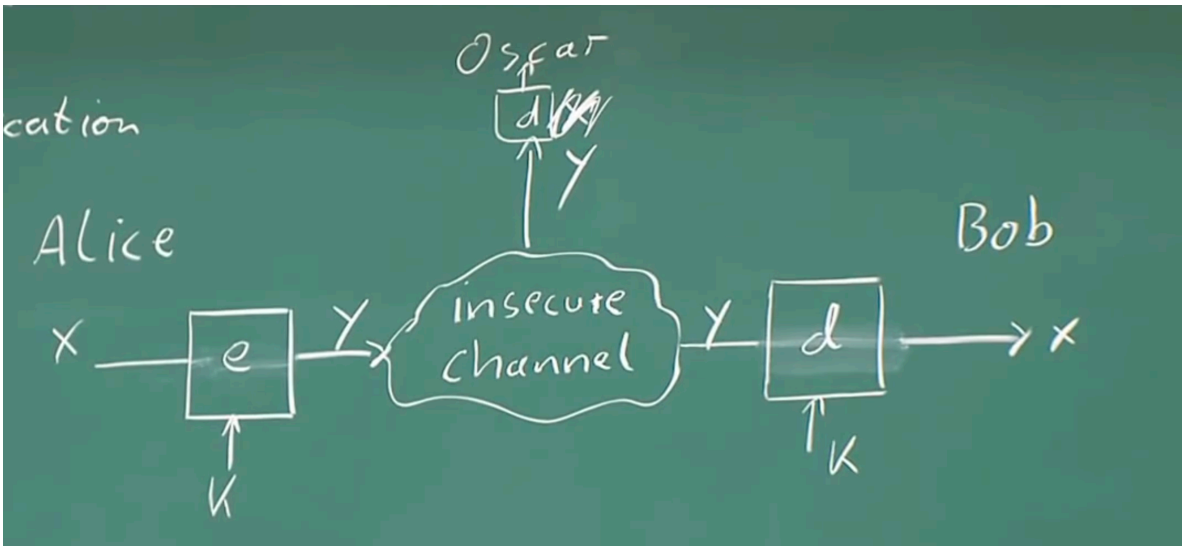
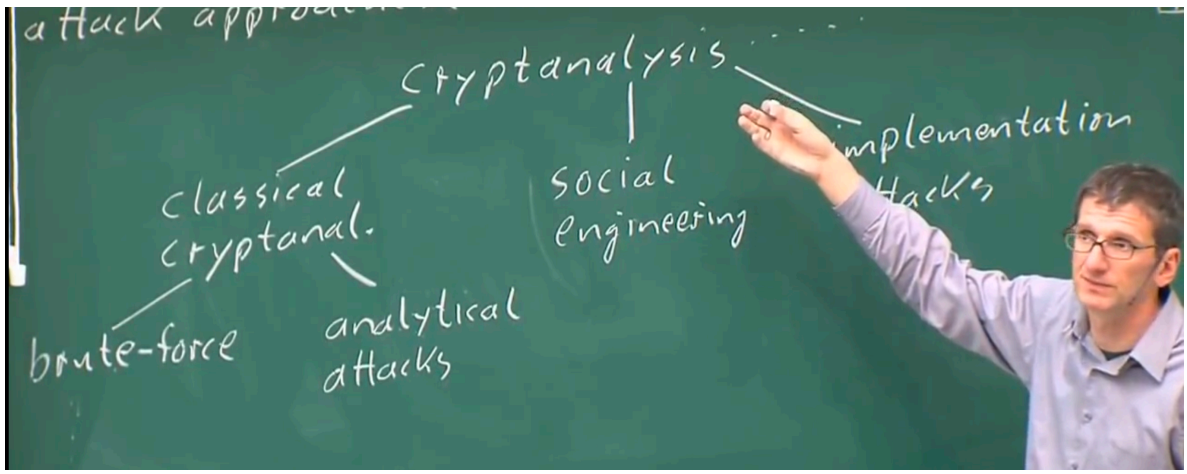
Lecture 1 Introduction to Cryptography

1. Applications of Cryptography :-
    1. Secure Shell
    2. Email Encryption
    3. Cell Phone(GSM Voice Encryption)
    4. Bank Cards
    5. VPN
    6. E-Passport
    7. Online Banking
    8. I-Tune, Copyright
    9. Kindle
2. **Question. How kindle uses Cryptography ?**
3. **Question. How GSM uses Voice Encryption ?**
4. **Question. What does Chip on Card does? How encryption works in it ?**
5. Channels :-
    1. Internet
    2. GSM Airwaves
    3. Wifi
6. Should we keep Encrypt and Decrypt Algorithms Secrete ?
    1. Until 1970, it was the idea to have E and D as Secrete.
    2. Question: Why now we need to make E and D Algorithm as Public?
        1. Everyone thinks they build the secure the E and D Algorithm.
        2. Only way of Assuring the E and D are secure is by Publicising it.
        3. CryptoAnalysis will try to break and if not able to do that then it can be regarded Secure.



    3. In Few instances, there is no mathematical proof that the Algorithm is secure and only way we have marked Secure is by telling that no one is able to break it till now.
    4. Breaking System, Basic way is Brute Forcing the Keys.

5. Kerckhoff's Principle
    1. Attacker knows everything about the System exception is Key.
    2. Very different way of thinking and it is counter intuitive.
6. Substitution Cipher :-
    1. Historical Cipher.
    2. Operate on Letters
    3. Idea : Replace Every PlainText letter with a Fixed Cipher Text Letter.
    4. A —> L, B —> D, C —> W
       e(ABBA) —> LDDL
7. Is this Cipher Secure ? No. Why/How can we attack this Cipher ?
    1. Brute Force :-
        1. KeySpace, In general StreamCiphers we check the KeySpace by Counting the Bits and raising to power of 2. In this Case it is little tricky. How many table we can compute ? For Letter A we have 26 possibilities and for B we have 25 and similarly 26! ~ 2^88. Very tough to compute 2^88.
        2. KeySpace is very Large so we cannot do the brute force attack.
    2. Letters are not equally likely in languages.
        1. You can do Letter frequency analysis.
        2. As 13% is the frequency of E and incase in cipher text you found a letter with probability of 13% then you can get that it is a E.
        3. Letters found in pairs or triples or quadruples like QU in English might help in breaking above cipher.
        4. If we assume word separators (spaces) have been found then we can use frequent short words like AND and THE etc. which can further weakens above encryption.
8. Learning from above :-
    1. Check against every kind of Attack.
    2. Classification of Attacks:-
        1. There are often many possible attack approaches ("Attack Vectors")



Lessons learned :- Good ciphers should hide the statistical properties of the encrypted plaintext. The ciphertext symbols should appear to be random. Also, a large key space alone is not sufficient for a strong encryption function.