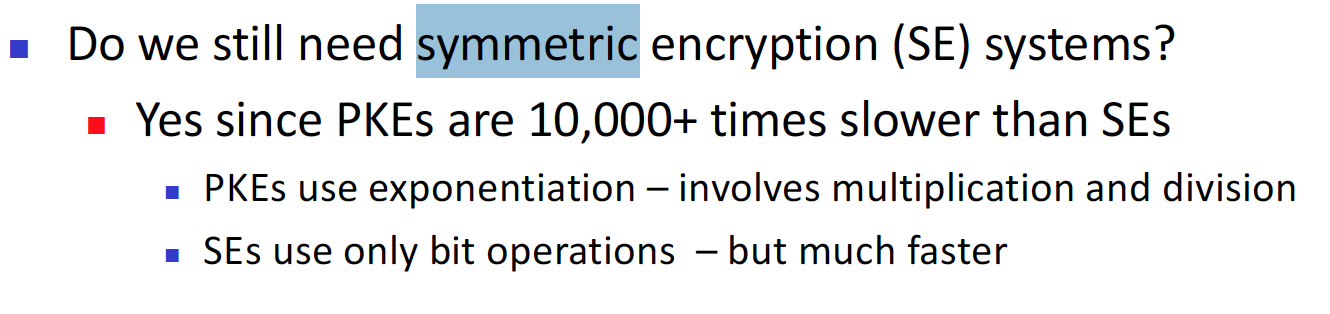
|  |  |  |
| --- | --- | --- |
|  |  | CPS 633 – note questions  Jae Duk Seo |

# Lecture 4 – Cryptography Applications

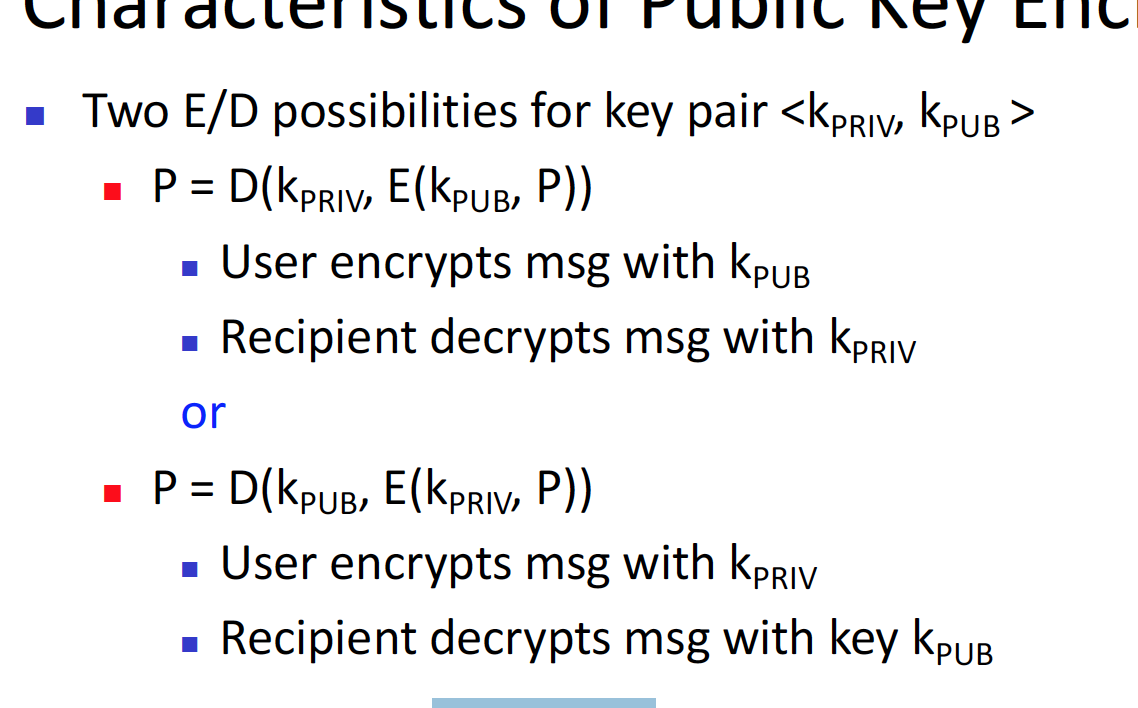
1. Why do we still need symmetric encryption?
2. What is PKE – public Key Encryption and why do we need this?
3. What is the requirement for PKE?
4. How can we achieve both confidentiality and integrity using PKE?
5. What is message authentication and why do we need this? Also tell me the steps of how to achieve message authentication.
6. What is a hash function?
7. Steps for hash function with encryption? (Tell me step by step.)
8. Describe the type of PKE algorithms.
9. How does RSA algorithm work and why is it hard to break?
10. What is check sum and what is partial check sum?
11. Difference between keyless and keyed checksum?
12. What is chaining mode?
13. Describe the steps to derive a symmetric key using PKE. – Why do we need this?
14. What is digital signature and how can we make the digital signatures?
15. Why do we need certificates and what is organization hierarchical structure?
16. What is the structure of t PKE, and how does it work?

# Lecture 4 – solUtions

1. Why do we still need symmetric encryption?

* We still need symmetric encryption since asymmetric encryption are expensive and computationally takes a longer time to process. (For easy task it is better to use the symmetric key)

1. What is PKE – public Key Encryption and why do we need this?

* This is a way to exchange keys between two host securely. This is achieved via the way how the PKE operates. The private key of an individual is inverse of its public key. So host A can use public key of B to encrypt the data, and B can use its private key to decrypt the data.

1. What is the requirement for PKE?
2. How can we achieve both confidentiality and integrity using PKE?
3. What is message authentication and why do we need this? Also tell me the steps of how to achieve message authentication.
4. What is a hash function?
5. Steps for hash function with encryption? (Tell me step by step.)
6. Describe the type of PKE algorithms.
7. How does RSA algorithm work and why is it hard to break?
8. What is check sum and what is partial check sum?
9. Difference between keyless and keyed checksum?
10. What is chaining mode?
11. Describe the steps to derive a symmetric key using PKE. – Why do we need this?
12. What is digital signature and how can we make the digital signatures?
13. Why do we need certificates and what is organization hierarchical structure?
14. What is the structure of t PKE, and how does it work?