CS 428 – Applied Cryptography

Module 8 Activity

Cameron Stark

1.) What are the three problems with private key encryption that we discussed today? Describe the two relating to the key.

* Key-Distribution
* Key-Management
* Lack of support for open-systems

2.) What is an open system?

* Two users who have never met each other or would have never exchanged keys before.

3.) What is asymmetry as described loosely by the book?

* Easy to compute, but hard to invert (such as factoring, RSA, etc.)

4.) What is authenticated key exchange?

* Key exchange is secure against passive eavesdropping
* Unable to compute the key given the transcript, cannot be guaranteed
* Indistinguishability of the shared key from uniform is a much stronger guarantee

5.) Explain the Diffie Hellman key exchange.

* A form of key exchange that works to prevent the ability for someone to passively eavesdropping

6.) What is public key setting?

* Public key is widely disseminated
* Private key is kept secret and shared with no one

7.) How is secrecy and integrity handled for both the private and public key setting?

* Private key setting
  + Secrecy – Private Key Encryption
  + Integrity – Message Authentication Code
* Public key setting
  + Secrecy – Public Key Encryption
  + Integrity – Digital Signature Schemes

8.) Explain how public key encryption combats the three drawback of private key encryption.

* Key Distribution
* Key Management in large systems
* Applicability in “open systems”

9.) What are the three polynomial time algorithms for public key encryption?

* Consists of three PPT algorithms
  + Gen – Key Generation
  + Enc – Encryption
  + Dec – Decryption

10.) Under CPA security what are two attacks the attack could run?

* Chosen-ciphertext attack
* Ciphertext malleability

11.) Why is chosen cipher text attacks and malleability a bigger deal for public key encryption?

* Because the public key setting, the key is widely distributed among parties and can easily be intercepted by an eavesdropper

12.) Why is the El Gamal encryption scheme not CCA secure?

* Because it suffers from being malleable which means that the ciphertext can be transformed to obtain information

13.) Why shouldn’t the plain RSA encryption scheme be used?

* It is deterministic, therefore not CPA secure
* Information may be leaked
* Information from cipher can be recovered
* Cipher is not uniform