**CHƯƠNG 1. Tổng quan về an toàn thông tin**

1. Các mục tiêu của an toàn thông tin:

* Tính bí mật (Confidentiality)
* Tính toàn vẹn (Integrity)
* Tính sẵn sàng (Availability)
* Tính xác thực (Authenticity)
* Tính trách nhiệm (Accountability)

Đặc điểm và ví dụ minh họa.

Liên hệ giữa các mục tiêu an toàn với một một số hình thức tấn công mạng, mã độc như Cryptojacking, DDOS, SQL Injection,Ransomware

3. Phân biệt điểm hở (vulnerability) và mối đe dọa (threat). Các rủi ro an toàn thông tin mạng.

2. Tấn công chủ động, bị động? Đặc điểm của mỗi loại, ví dụ minh họa?

**CHƯƠNG 2. Các khái niệm cơ sở và mật mã khóa đối xứng**

1. 5 thành phần cơ bản của một hệ mã?

2. Phân loại hệ mã? Đặc điểm của từng loại

3. Đặc điểm chung của mật mã khóa đối xứng? Mô hình liên lạc bí mật sử dụng mật mã khóa đối xứng?

4. Phân biệt hệ mã chuyển vị và thay thế?

5. Phân biệt hệ mã thay thế đơn biểu và đa biểu? Tên các hệ mã thay thế đơn biểu, đa biểu đã học.

6. Phân biệt mã dòng và mã khối? Tên một số hệ mã dòng, mã khối đã học.

7. Đặc điểm của tấn công thám mã và tấn công vét cạn?

8. Các kiểu tấn công thám mã? Đặc điểm của mỗi loại?

----------------------------------------------------

9. Hệ mã Caesar: 5 thành phần của hệ mã. Giải bài tập, ví dụ.

10. Hệ mã Playfair: 5 thành phần của hệ mã. Giải bài tập, ví dụ.

11. Hệ mã Hill: 5 thành phần của hệ mã. Giải bài tập, ví dụ.

12. Hệ mã Vigenere: 5 thành phần của hệ mã. Giải bài tập, ví dụ.

13. Hệ mã One-Time Pad: 5 thành phần của hệ mã. Giải bài tập, ví dụ.

------------------------------------------------------------------------------------

14. Nêu một số ứng dụng thực tiễn sử dụng mã dòng RC4 và A5/1

15. Các hệ mã khối được thiết kế theo kiến trúc mạng SPN nhằm đạt tính khuếch tán và tính gây lẫn? Đặc điểm của 2 tính chất này là gì? Phân biệt chúng.

16. Hệ mã DES: Phân tích và hiểu rõ 5 thành phần của hệ mã?

17. Hiện tượng hiệu ứng tuyết lở trong hệ mã DES là gì?

18. Hệ mã AES: Phân tích và hiểu rõ 5 thành phần của hệ mã? Các phép biến đổi được thực hiện trong hệ mã (SubBytes, Shiftrows, Mixcolumns, Addroundkey) và ý nghĩa của chúng?

**CHƯƠNG 3. Mật mã khóa công khai**

19. Ưu điểm của mật mã khóa công khai so với với mật mã khóa đối xứng?

20. Đặc điểm chung và mô hình liên lạc bí mật sử dụng mật mã khóa công khai?

21. Các ứng dụng của mật mã khóa công khai? (mã hóa/giải mã; ký số, trao đổi khóa)?

22. Nêu các hàm toán học một chiều được áp dụng trong các hệ mã khóa công khai đã học?

23. Hệ mã RSA: Phân tích và hiểu rõ 5 thành phần của hệ mã? Các thuật toán được sử dụng để tính toán các thành phần trong hệ mã. Giải bài tập, ví dụ.

24. Hệ mã Diffie-Hellman: Phân tích và hiểu rõ 5 thành phần của hệ mã? Các thuật toán được sử dụng để tính toán các thành phần trong hệ mã. Giải bài tập, ví dụ.

25. Hệ mã Elgamal: Phân tích và hiểu rõ 5 thành phần của hệ mã? Các thuật toán được sử dụng để tính toán các thành phần trong hệ mã. Giải bài tập, ví dụ.

26. So sánh hệ mã RSA và hệ mã đường cong Ellipt?

27. Hệ mã đường cong ellipt: Phân tích và hiểu rõ 5 thành phần của hệ mã? Giải bài tập, ví dụ.

**CHƯƠNG 4. Hàm băm và chữ ký số**

28. Các tính chất của hàm băm mật mã? Mục đích sử dụng hàm băm mật mã?

29. Hàm băm mật mã được sử dụng trong sơ đồ ký số như thế nào?

30. Kẻ tấn công có thể lợi dụng điểm yếu nào của hàm băm để thực hiện tấn công vét cạn?

31. Kẻ tấn công có thể lợi dụng điểm yếu nào của hàm băm để thực hiện tấn công thám mã?

32. Các phiên bản băm SHA? Đặc điểm chung của từng loại.

33. Phân tích và làm rõ các thành phần của thuật toán băm SHA-512

34. Phân tích và làm rõ các thành phần của thuật toán băm SHA-3

-------------------------------

35. 3 thành phần của chữ ký số?

36. Các yêu cầu đối với chữ ký số?

37. Các kiểu tấn công và giả mạo chữ ký số?

38. Phân tích và hiểu rõ 3 thành phần của sơ đồ ký số Elgamal? Giải bài tập, ví dụ.

39. Phân tích và hiểu rõ 3 thành phần của sơ đồ ký số Schnorr?

40. Phân tích và hiểu rõ 3 thành phần của sơ đồ ký số NIST - DSA?

41. Phân tích và hiểu rõ 3 thành phần của sơ đồ ký số đường cong Ellip?

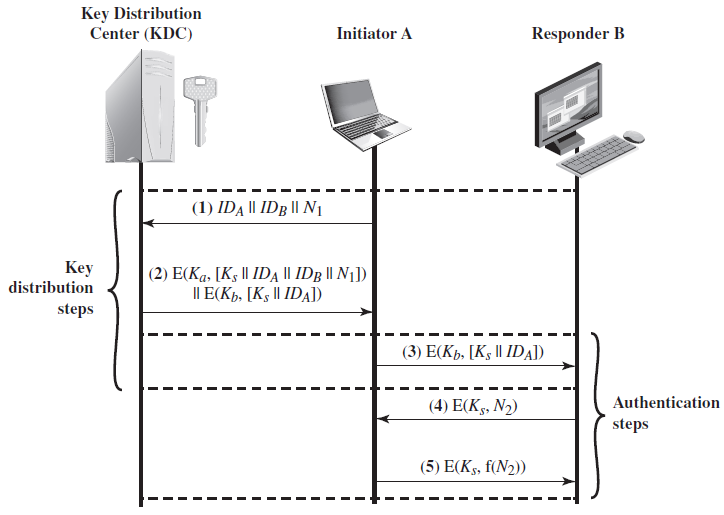
42. Phân tích và hiểu rõ 3 thành phần của sơ đồ ký số RSA-PSS?

**CHƯƠNG 5. Quản lý và phân phối khóa**

43. Các thức một thực thể A có thể phân phối bí mật sang cho thực thể B sử dụng mật mã khóa đối xứng? Trong các cách này thì cách nào có thể sử dụng cho mã hóa đầu cuối tới đầu cuối (end-to-end)?

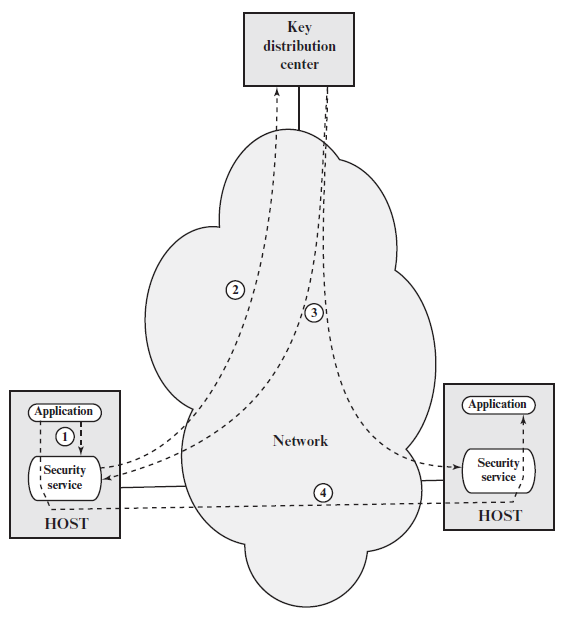
43. Trong sơ đồ phân cấp khóa của hệ thống phân phối khóa cho mã hóa end-to-end, khóa phiên (session key) và khóa chính (Master key) được sử dụng để làm gì? Số lượng khóa phiên và khóa chính cần phân phối trong sơ đồ gồm N host là bao nhiêu?

44. Phân tích và hiểu rõ sơ đồ phân phối khóa sau (gồm các thành phần gì, hoạt động phân phối khóa diễn ra như thế nào..)?

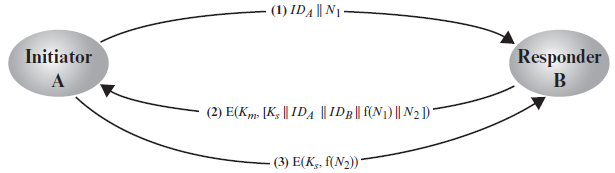


45. Vòng đời của khóa phiên được xác định như thế nào?

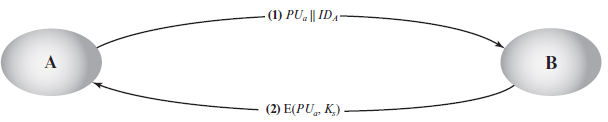
46. Phân tích và hiểu rõ sơ đồ quản lý khóa trong suốt với user



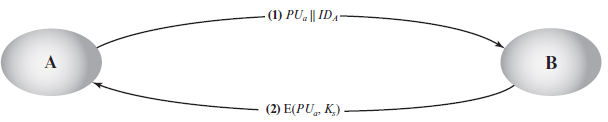
47. Phân tích và hiểu rõ sơ đồ phân phối khóa không tập trung (không sử dụng KDC) sau:

------------------------------

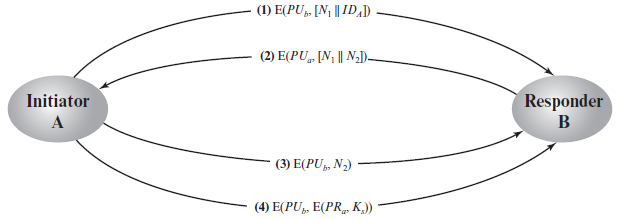
48. Phân tích và hiểu rõ sơ đồ phân phối khóa sau, ưu/nhược điểm của nó?



49. Tấn công người ở giữa (man-in-the-middle) xảy ra như thế nào với sơ đồ phân phối khóa sau:



50. Phân tích và hiểu rõ sơ đồ phân phối khóa bí mật đảm bảm tính bí mật và xác thực sau:

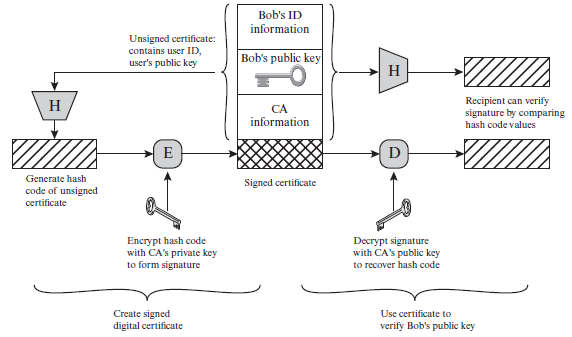


51. Các hình thức phân phối khóa công khai? Đặc điểm của mỗi loại, ưu, nhược điểm?

52. Chứng chỉ số X.509

52.1. Đặc điểm chung về chứng chỉ số X.509?

52.2. Phân tích sơ đồ X.509 tạo và xác minh chứng chỉ công khai:



52.3. Định dạng chung của chứng chỉ số X.509?

52.4. Người dùng lấy chứng chỉ số X.509 như thế nào? Thu hồi chứng chỉ số được thực hiện như thế nào?khi nào thì thu hồi?

53. Cơ sở hạ tầng khóa công khai PKI là gì?Mục tiêu chính phát triển PKI?