Trac nghiem 54 cau atm final linhnm 4297

Introduction of information security (Trường Đại học Bách khoa Hà Nội)

Tr c nghi m 54 câu

1. Mã hóa là gì ?
) t p h p các ph ng pháp và ph ng ti n b o v thông tin kh i vi c truy c p trái phép b ng cách n y u t t n t i các thông tin bí m t.
b) môn khoa h c v các ph ng th c bi n đ i (mã hóa) thông tin v i m c đích b o v thông tin kh i ng i truy c p trái phép
c) môn khoa h c (và th c t ng d ng nó) v các ph ng pháp và ph ng th c gi i mã

2. Steganography là gì ?
) b o v thông tin kh i truy c p trái phép b ng cách n đi s t n t i các thông tin bí m t
b) n đi n i dung c a tin b ng cách mã hoá chúng
c) ph m vi ki n th c ,mà m c đích c a nó là tìm ki m và nghiên c u các ph ng pháp b khóa các thu t toán mã hóa ,cũng nh là th t c b khóa

3. H th ng mã hóa Vizhiner thu c l p bi n đ i nào?
) hoán v **b) phép th** c) Gamma Xoring d) mã hóa kh i

4. Mã Sejar thu c l p bi n đ i nào ? (Ceasar ch ko ph i Sejar)
) phép th b) phép hoán v c) gama xoring

5. Mã thay th (substitution cipher) là gì ?
) m t mã lu ng mà đó Gamma xoring đ c s d ng đ mã hóa d li u ?
b) m t mã ,mà đó th t c mã hóa là s hoán v các ph n t c a văn b n ban đ u ho c các nhóm c a chúng, b n thân các ph n t gi nguyên không thay đ i
c) m t mã,mà đó các ký t riêng r c a văn b n ban đ u ho c nhóm các ký t đ c thay th b i các ký t ho c nhóm các ký t khác, trong khi gi nguyên v trí c a mình so v i các nhóm đ c thay th khác

6. Mã hoá Gamma Xoring là gì?
) m t mã lu ng mà đó b c m bi n c a các s gi ng u nhiên đ c s d ng đ mã hóa d li u
b) m t mã mà đó th t c mã hóa là s hoán v các ph n t c a văn b n ban đ u ho c nhóm các ph n t ,b n than các ph n t thì không thay đ i
c) m t mã mà đó các ký t riêng r c a văn b n ban đ u ho c nhóm các ký t đ c thay th b i các ký t ho c nhóm các ký t khác , tro ng khi gi v trí c a chúng trong văn b n so v i các nhóm b thay th khác

7. Nh ng thu t toán nào sau đây là thu t toán đ i x ng ?
) DES b) El-Gamal **c) RC5 d) IDEA**

8. Thu t toán nào sau đây không ph i là đ i x ng ?
) DES **b) El-Gamal** c) RC5 d) IDEA

9. Chìa khóa m t trong h mã hoá DES có đ dài là bao nhiêu ?

) 48 bit;
b) 64 bit; - có b n đã tr l i r i 56 bit đ mã hóa, 8 bit đ ki m tra parity
c) 128 bit; d) 192 bit; e) 256 bit

10. Chìa khóa m t trong h mã hóa Rijdael có đ dài b ng bao nhiêu? (aka Advanced Encryption Standard (AES))

Key sizes	128, 192 or 256 bits[1]
Block sizes	128 bits[2]
Structure	Substitution-permutation network
Rounds	10, 12 or 14 (depending on key size)

) 48 bit; b) 64 bit; **c) 128 bit; d) 192 bit; e) 256 bit.**

11. Thu t toán Rijndael có ki n trúc nào ?
) m ng Filestel b) m t mã lu ng (stream cipher)
c) ki n trúc SQUARE (_http://en.wikipedia.org/wiki/Advanced_Encryption_Standard)

12. Thu t toán DES có ki n trúc nào?
) m ng Filestel b) mã lu ng (stream cipher) c) ki n trúc SQUARE

13. Đ c tính đ c bi t c a các thu t toán m hóa kh i là :
) trong quá trình làm vi c ,chúng bi n đ i kh i thông tin ban đ u có đ d ài xác đ nh và nh n đ c kh i k t qu v i đ dài b t kỳ
b) trong quá trình làm vi c ,chúng bi n đ i kh i thông tin ban đ u v i đ dài xác đ nh và nh n đ c kh i k t qu v i đ dài t ng t
c) trong quá trình làm vi c ,chúng bi n đ i kh i thông tin ban đ u v i đ d ài b t kỳ và nh n đ c kh i k t qu v i đ dài xác đ nh

14. ECB (Electronic Code Book), CBC (Cipher Block Chaining), OFB (Output Feed Back), CFB (Cipher Feed Back) là gì?
) là nh ng ch đ làm vi c c a thu t toán DES
b) là nh ng ch đ làm vi c c a thu t toán RSA
c) là nh ng ch đ làm vi c c a thu t toán Rijndael

15. C s c a đ b n c a thu t toán RSA là?
) s phân tích các s l n thành các th a s nguyên t (đ c l i v ghi r t rõ)
b) tính lôgarit t i tr ng h u h n
c) tính nghi m c a các ph ng trình đ i s

16. C s c a đ b n c a ph ng pháp Diff-Hellman là :

) phân tích các s l n thành các th a s nguyên t
b) hàm nâng lên lũy th a r i r c (thu t toán logarit r i r c)
c) tính nghi m c a các ph ng trình đ i s

17. Thành ph n nào c a c s h t ng c a khóa m (PKI – Public Key Infrastructure) ch u trách nhi m vi c t o danh sách ch ng nh n b thu h i ?
) trung tâm ch ng nh n c) ng i s d ng cu i cùng
b) trung tâm đăng ký d) c m nang tra c u m ng

18. C s h t ng c a khóa m (Public Key Infrastructure – PKI) đ c s d ng đ làm gì ?
) đ đi u khi n các chìa khóa m t c a nh ng thành ph n tham gia t ng tác
b) đ đi u khi n các khóa và ch ng th c đi n t c a nh ng thành ph n tham gia t ng tác

19 – Giao th c nào đ c xây d ng đ đ m b o vi c b o m t cho h òm th đi n t ?
a) S/MINE - (Secure/Multipurpose Internet Mail Extension s)
b) SET
c) IPSEC

20. Giao th c nào đ c xây d ng đ đ m b o cho h th ng thanh toán đi n t c a ngân hàng v i vi c s d ng th plastic ?
) S/MIME
b) SET - Secure Electronic transaction – Thanh toán đi n t an toàn
c) IPSEC

21. Th t c phân b khóa (key) mà không yêu c u s d ng kênh b o m t đ i v i vi c truy n khóa đ n ng i nh n là th t c :
) mã hóa theo thu t toán DES
b) Diff - Hellman (mã công khai)
c) mã hóa Vizhiner

22. Th t c phân b c a khóa nào yêu c u s d ng kênh b o m t đ truy n khóa t i ng i nh n ?
) th t c phân b khóa đ i x ng – ví d DES
b) th t c Diff-Hellman

23. Nh ng tính ch t nào là tính ch t c n thi t đ i v i h th ng không đ i x ng b t kỳ ?
a) s t n t i kênh đóng đ truy n các khóa(key) bí m t
b) không th đ c thông đi p,ch bi t khóa m (khóa m - public key – bi t là đ ng nhiên, ko đ c đ c thì m i m t)
c) không th tính khóa đóng theo khóa m (tính đ c còn g i gì là m t)

24. Th t c mã hóa nào sau đây có năng su t h n ?
) mã hóa không đ i x ng (yêu c u năng l c tính toán ph c t p)

b)mã hóa đ i x ng

25. H th ng v i khóa m nào sau đây có năng su t nh t ?
) h th ng RSA
b) h th ng El-Gammal
c) h th ng trên c s các đ ng cong êlip

26. H th ng v i khóa m nào sau đây đ c s d ng ch đ sinh ra ch ký s ?
) RSA b) Diffs-Hellman c) ECC
d) El-Gamal
e) DSS – ch đ sinh ch ký s nên ch n th ng này

27. H th ng v i khóa m nào sau đây có hi u su t l n nh t ?
) nh ng h th ng, đ c xây d ng trên c s phân tích các s l n thành các th a s nguyên t
b) nh ng h th ng , đ c xây d ng trên c s tính lôgarit r i r c trong tr ng h u h n
c) nh ng h th ng, đ c xây d ng trên c s các đ ng cong elip
http://www.tapchibcvt.gov.vn/News/PrintView.aspx?ID=16382

28. Nh ng h th ng v i khóa m nào sau đây đ c s d ng đ mã hóa thông tin ?
) RSA
b) Diff-Hellman - th ng này dùng đ trao đ i khóa
c) El-Gamal – th ng này ch ký s
d) DSS – th ng này ch ký s

29 . Thu t toán RSA thu c d ng nào c a thu t toán mã hóa (xét trên ph ng di n đ ch c ch n khi b b khóa) ?

) hi n nhiên ch c ch n – h m t hoàn h o
b) ch c ch n đ c ch ng th c – đ ph c t p tính toán
c) ch c ch n gi đ nh

30. Thu t toán Vernam (s ghi chép 1 l n) thu c d ng n ào c a thu t toán mã hóa (xét trên ph ng di n đ ch c ch n khi b b khóa)?
) hi n nhiên ch c ch n
b) ch c ch n đ c ch ng th c
c) ch c ch n gi đ nh (thuy t)

31. Đi u gì quy t đ nh đ tin c y c a thu t toán DES?
) phân tích các s l n thành các th a s nguyên t ;
b) kích th c c a khóa;
c) tính nghi m c a các ph ng trình đ i s .

32. C s c a đ ch c ch n c a ph ng pháp El-Gamal là :
a) S phân tích các s l n thành các th a s nguyên t
b) Tính lôgarít trong tr ng h u h n – cùng lo i v i Diffie-Hellman, Knapsach

c) Tính nghi m c a các ph ng trình đ i s

33. Ph ng pháp nào sau đây không th đ c s d ng đ mã hóa hay gi i mã thông tin?
) ph ng pháp BlowFich
b) ph ng pháp El-Gammal
c) ph ng pháp Diff-Hellman

34. Message digest – là …
) k t qu c a vi c mã hóa;
b) k t qu c a hàm hash ;
c) k t qu c a vi c gi i mã

35. Th t c ch ng th c (authentication) d li u l à gì ?
) th t c ki m tra tính toàn v n c a d li u
b) th t c ki m tra tính đúng đ n c a d li u v à các ch th t ng tác thông tin
c) th t c đ m b o vi c b o v d li u kh i vi c truy c p trái phép

36. Ch ký đi n t (s) là :
) các đ c tính c a m t mã, đ c s d ng đ bi n đ i mã hóa thông tin
b) h tên ng i g i đ c ghi d ng đi n t v à k t n i v i thông tin
c) bi n đ i mã hóa văn b n đ c g n vào văn b n cho phép ng i nh n khác ki m tra tác gi và tính đích th c c a thông tin

37. K t qu c a phép tính h àm hash theo thu t toán MD5 b ng bao nhi êu ?
) 64 bit **b) 128 bit** c) 160 bit d) 256 bit

38. Hàm hash là gì ?
) là s bi n đ i, nh n giá tr nào đó có đ dài b t kỳ t d li u có đ dài c đ nh
b) là s bi n đ i, nh n giá tr n ào đó có đ dài c đ nh t d li u có đ dài b t kỳ
c) là s bi n đ i, nh n các giá tr khác có đ d ài b t kỳ t d li u có đ dài b t kỳ

39. Hàm hash 1 phía là gì ?
) hàm hash, khó tính theo h ng thu n và d tính theo h ng ng c
b) hàm hash , d tính theo h ng thu n và h ng ng c
c) hàm hash, v m t tính toán là hàm không thu n ngh ch -
kythuatmatma.com/lythuyet/congkhai/1002_ham1chieu.php

40. K t qu c a phép tính hàm hash theo thu t toán SHA-1 là?
) 64 bit b) 128 bit **c) 160 bit** d) 256 bit

Input: Đ u vào message có đ dài < 2^{64}, chia thành các block có size 512 bit
Output: 1 digest có đ dài 160 bit
B o m t:

- Ko tính ra đ c thông đi p v i 1 digest đã cho
- Ko có 2 message t o ra cùng 1 digest

41. Mã nào sau đây là mã không đ i x ng?
) DES (Data Encryption Standart)
b) RSA (Rivest-Shamir-Alderman)
c) El Gamal
42. Nh ng mã nào sau đây là đ i x ng?
) DES (Data Encryption Standart)
c) chu n 28147-89 – hay là GOST (block cipher)
b) RSA (Rivest-Shamir-Alderman) d) El Gamal

43. Nh ng thu t toán nào đ c s d ng đ tính toán digest thông tin ?
) DES
b) MD5 V c) SHA-1 - xem câu 34
d) RSA

44. Nh ng thu t toán nào sau đây không đ c s d ng đ tính toán digest thông tin?
) DES b) MD5 c) SHA-1 **d) RSA**

45. Khi nào thì c n đ a t ng l a vào trong thành ph n trang thi t b c a c quan
) khi liên k t ngu n tính toán c a c quan vào m ng n i b
b) khi mua h th ng phòng ch ng virus
c) khi th ng xuyên k t n i th ng t m ng n i b ra m ng internet

46. Nh ng nguy c nào yêu c u đ a t ng l a vào thành ph n trang thi t b cu c quan
) nh ng nguy c xâm nh p trái phép vào m ng n i b t m ng bên ngoài
b) nh ng nguy c truy c p trái phép vào m ng bên ngoài t m ng bên trong
c) nh ng nguy c xu t hi n l i c a ng i s d ng,ng i đi u ph i và ng i qu n lý

47. T ng l a th c hi n nh ng ch c năng n ào sau đây ?
a) ch c năng l c nh ng lu ng thông tin đi qua
b) ch c năng trung gian khi th c hi n các t ng tác gi a các m ng
c) (hàm) ch c năng bi n đ i mã hóa các lu ng thông tin

48. Nh ng bi n đ i mã hóa nào sau đây đ c s d ng đ mã hóa thông tin khi xây d ng " phong bì đi n t "?
a) các thu t toán mã hóa đ i x ng
b) các thu t toán mã hóa không đ i x ng

49. Vi c b o v thông tin trong quá trình truy n theo kênh liên k t m đ c xây d ng trên c s th c hi n :
a) (hàm) các ch c năng b o v mã hóa c a d li u đ c truy n
b) (hàm) các ch c năng b o v vi c k t n i m ng n i b ho c các máy tính cá nhân t i kênh công c ng kh i các tác đ ng trái phép t môi tr ng bên ngoài

50. M ng riêng o (VPN) th c hi n nh ng bài toán nào sau đây ?
) b o v nh ng m ng n i b và các máy tính cá nhân có k t n i t i kênh công c ng kh i các tác đ ng trái phép t môi tr ng bên ngoài
b) b o v thông tin trong quá trình truy n theo các kênh liên l c m

51. "Ch ng trình cài vào " là gì ?
) là ch ng trình đ c xây d ng đ t đ ng th c hi n các tác đ ng trái phép
b) là ch ng trình dùng đ b o v b ng mã hóa d li u kh i s truy c p trái phép

52. "Ch ng trình cài vào " đ c cài vào b i các công c ph n c ng nh th nào?
a) b i các ch ng trình b lây nhi m d ng b t kỳ theo công ngh virus
b) b ng cách lây nhi m c a các ch ng trình ch a trong các công c ph n c ng, ví d các ch ng trình c a vi m ch BIOS …

53. Gi i mã là :
) t p h p các ph ng pháp và môi tr ng đ khôi ph c l i các thông tin đã b mã hóa tr l i d ng ban đ u mà không c n khóa c n thi t.
b) khôi ph c các thông tin đã b mã hóa l i d ng ban đ u v i s giúp đ c a khóa t ng ng.

54. Phân tích mã là:
) T p h p các ph ng pháp và công c đ th c hi n vi c gi i mã thông tin mà không c n có chìa khóa c n thi t
b) khôi ph c thông tin l i m u ban đ u v i s giúp đ c a khóa t ng ng

55. L c các lu ng thông tin b i t ng l a là :
) l c l ng thông tin cho thông tin qua t ng b o v có ch n l c kèm theo th c hi n 1 vài s bi n đ i.
b) l c l ng thông tin (có trong d li u) là bi n đ i mã hóa d li u đi qua t ng l a.