UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO TECNOLÓGICO
DEPARTAMENTO DE INFORMÁTICA E ESTATÍSTICA

Disciplina: INE 5680 – Segurança da Informação e de Redes
Professora: Carla Merkle Westphall

Exercícios

1. Quais as três características essenciais de segurança? Cite um exemplo prático de cada característica.
2. Cite e explique três tipos importantes de ataques feitos na Internet.
3. Qual a diferença entre ataque ativo e ataque passivo – cite um exemplo de cada tipo.
4. Em qual nível das camadas da rede devem ser implementados mecanismos de segurança? Explique.
5. O que é uma vulnerabilidade? Conceitue e cite um exemplo.
6. Usando a base NVD (http://nvd.nist.gov/), encontre a mais recente vulnerabilidade do navegador Internet Explorer ou servidor Web Apache e apresente:
   a) código CVE;
   b) explicação da vulnerabilidade;
   c) possíveis soluções, caso uma atualização do software não seja possível ou viável.
7. As vulnerabilidades são geralmente classificadas usando CVSS (*Common Vulnerability Scoring System*). Explique o que é CVSS (https://www.first.org/cvss/) e como ele é construído.
8. Pesquise o uso das normas da família ISO 27000:
   a) Cite como são usadas as normas ISO 27001 e ISO 27002.
   b) Qual o motivo que obriga uma empresa a usar essas normas?
   c) Procure uma política de segurança de alguma empresa brasileira e cite o link do documento da política aqui.
9. Consultando o seguinte documento sobre a situação da Segurança Cibernética no Brasil (http://www.ipea.gov.br/portal/images/stories/PDFs/TDs/td_1850.pdf) responda:
   a) O que significa Segurança Cibernética?
   b) O que foi o Stuxnet?
10. Descreva o que é o projeto OWASP.
11. Cite as três maiores ameaças em aplicações descritas em: https://www.owasp.org/images/0/06/OWASP_Top_10-2017-pt_pt.pdf
12. O que significa autenticidade? Cite um exemplo prático da necessidade de se garantir a autenticidade.
13. Conceitue criptografia.
14. Cite os dois tipos principais de algoritmos criptográficos.
15. Qual é o Princípio de *Kerckhoff*?
16. Quais são as técnicas de cifragem básicas?

17. Cifre o seguinte texto utilizando o cifrador de Vigenere: USAR DA FORMA CERTA. Utilize a tabela abaixo para a realização desta atividade e como chave a palavra CAVALO.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

18. Como pode ser feita a quebra das cifras de substituição?

19. Quais são as *entradas* de um algoritmo criptográfico? O que é necessário se ter para usar um algoritmo criptográfico?

20. Explique o funcionamento da criptografia simétrica usando a figura 1.

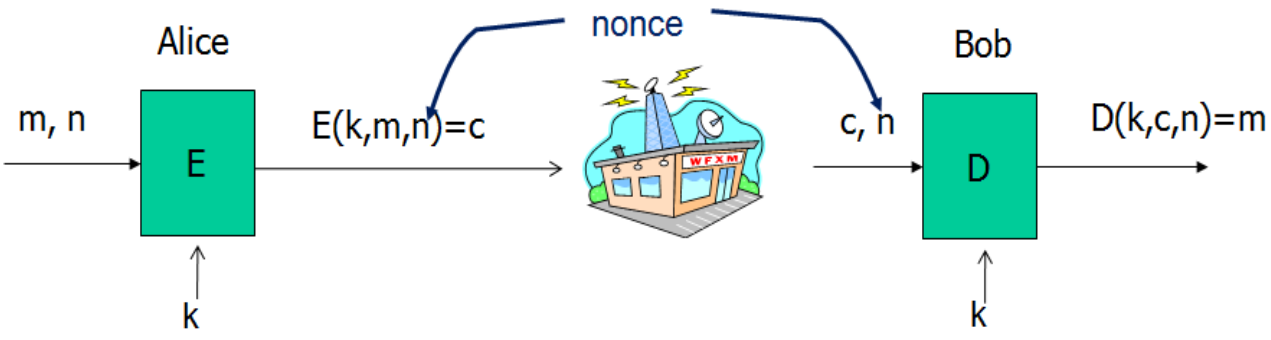


Figura 1 – Criptografia simétrica

21. Dê exemplos de algoritmos simétricos.

22. Qual a diferença entre chave de uso único e chave de uso múltiplo? Explique e comente.

23. Pesquise e responda: porque One Time Pad é “seguro” contra ataques de texto cifrado (*ciphertext-only attacks*)?

24. Usando o método “one time pad” para criptografar a mensagem "attack at dawn" gera o seguinte texto cifrado: *09e1c5f70a65ac519458e7e53f36* (as letras do texto plano são codificadas usando ASCII 8-bits e o texto cifrado é escrito em hexa). Supondo que a mesma chave one time pad é usada para cifrar a mensagem "attack at dusk", escreva qual é o texto cifrado (calcule manualmente).

25. Explique o que é uma cifra de fluxo. Cite nomes de algoritmos deste tipo.

26. Explique o problema do protocolo 802.11b WEP. Qual a cifra de fluxo usada no WEP?

27. Como foi feita a quebra do WPA2 em 2017? Veja os detalhes em https://www.krackattacks.com/ e nos slides.

28. Explique o que é uma cifra de bloco. Cite nomes de algoritmos deste tipo.

29. Como as cifras de bloco podem ser construídas pela iteração? Explique.

30. Mostre como funciona uma Rede Feistel (de forma resumida), tanto para cifrar quanto para decifrar.

31. Cite nomes de algoritmos que são baseados na Rede Feistel.

32. Descreva o esquema usado para a construção do AES-128. É uma Rede Feistel? (Obs.: O capítulo 5 do livro do Stallings, disponível no moodle, explica todos os detalhes sobre o AES.)

33. Descreva os tamanhos de bloco e tamanhos de chave dos algoritmos DES, 3DES e AES.

34. O que são os “modos de operação” das cifras de bloco?

35. Quais as desvantagens do modo ECB?

36. Como funciona a cifragem no modo CBC?

37. O que é o IV do modo CBC?

38. Para garantir a segurança no modo CBC, existe algum LIMITE de mensagens que podem ser cifradas com a mesma chave? Explique e dê exemplo.

39. A chave de um algoritmo de criptografia simétrica tem 3 bits. O IV tem 2 bits. Supondo que essa chave será usada para cifrar 35 mensagens:

    a) explique para que serve e como é usado o IV;

    b) considerando o uso do IV, explique quantas chaves diferentes podem existir;

    c) será possível cifrar todas as 35 mensagens e garantir a segurança contra ataques ao texto cifrado?

40. Para chaves de uso múltiplo e segurança contra ataques de texto plano, comente as duas formas de escolher o IV. O que significa IV único?

41. Como funciona o *padding* PKCS5?

42. Observando a figura 2, explique como funciona a cifragem no modo Counter (CTR). Leia também a seção 6.6 no livro do Stallings: https://moodle.ufsc.br/pluginfile.php/2838810/course/section/1284722/Criptografia%20e%20Seguranc%CC%A7a%20de%20Redes%20-%206%C2%AA%20Ed.%202014.pdf

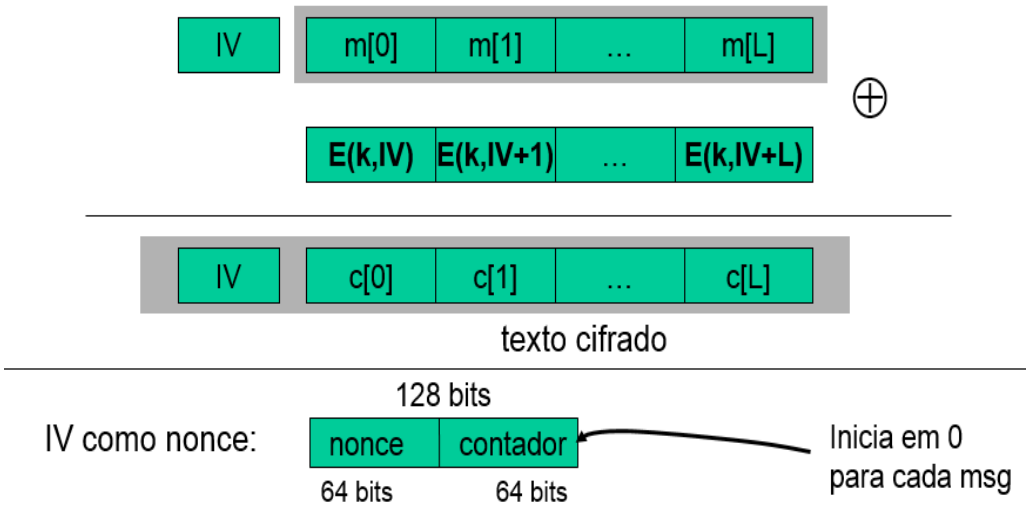


Figura 2 – Modo Counter (CTR)

43. Por que o modo *Counter* (CTR) é superior ao modo CBC?

44. Qual a vantagem e a desvantagem dos sistemas de criptografia simétrica?

45. Quais as propriedades das funções hash criptográficas?

46. Como funciona a construção Merkle-Damgard (base do SHA-1 e SHA-2)?

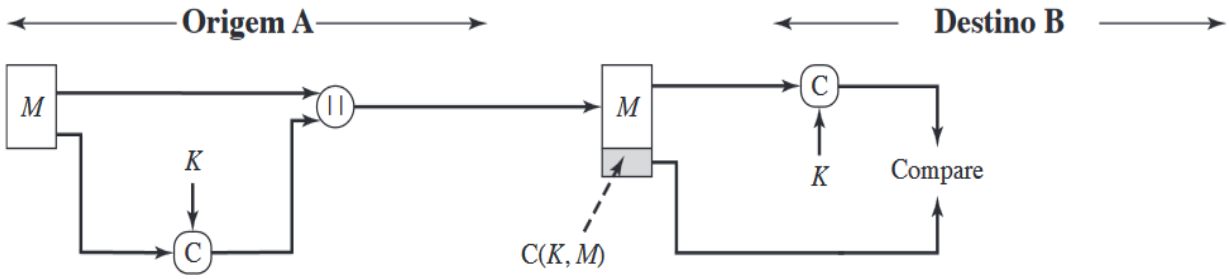
47. Explique o conceito de hash sem chave.

48. Explique o conceito de hash com chave. Por que o hash com chave fornece integridade e autenticidade?

49. Quais as duas formas de construir sistemas de MAC?

50. Explique em detalhes o funcionamento representado na figura 3. A figura 3(a) é igual à figura 3(b). Na figura 3(a), o cálculo do MAC é chamado de TAG. Na figura 3(b), o cálculo do MAC é chamado de C e é calculado assim: MAC = C(K, M). A figura 3(b) está no livro do Stallings. O MAC pode ser chamado de: mac, hash com chave, código de autenticação de mensagem e tag.

(a)



(b)

Figura 3 – MAC

51. Cite nomes de algoritmos de hash sem chave e com chave considerados importantes.

52. Considerando que um código Java de um programa envia pela rede a mensagem e o SHA-256 da mensagem, conforme representado na figura 4, responda:

a) É possível que um atacante consiga modificar ambos: a mensagem e o SHA-256 da mensagem? O receptor irá identificar a modificação? Explique.

b) Se o item a é possível, explique como impedir essa situação.

Mensagem	SHA-256 (Mensagem)

Figura 4 – Mensagem + SHA-256

53. De acordo com o link https://crackstation.net/hashing-security.htm, comente o que é certo e o que é errado quando se usa hashes (com salt) para guardar senhas.

54. Como o MAC pode ser usado para proteger o sistema de arquivos?

55. Qual a diferença entre o “raw CBC-MAC” e o ECBC (Encrypt CBC-MAC)? Qual dos dois é mais seguro e por que?

56. Como é feito o *padding* no CBC-MAC?

57. Como o CMAC (padrão NIST) se diferencia do ECBC?

58. Como funciona o HMAC? É um MAC construído com cifra de bloco ou com funções hash?

59. O que é criptografia autenticada (*authenticaded encryption*)?

60. Como é que a criptografia autenticada consegue garantir a confidencialidade, a integridade e a autenticidade? Explique.

61. Quais os modos de criptografia autenticada? Represente cada um dos modos com uma figura.

62. Quais os padrões de criptografia autenticada? Quais os padrões que a biblioteca *Bouncy Castle* implementa?

63. Por que existem formas de “derivação de chaves”?

64. O que é uma função KDF?

65. Por que as senhas não podem ser usadas diretamente como chaves?

66. Como funciona o PBKDF2? Quais os parâmetros necessários para o seu funcionamento?

67. Usando a notação descrita abaixo, suponha que A quer enviar uma mensagem M para B. As partes A e B compartilham uma chave simétrica K. Faça:

    a) Responda SIM ou NÃO em cada quadrado em branco;

    b) Se respondeu SIM em alguma opção você deve justificar COMO essa opção é oferecida.

Descrição da notação
Mac = C(K, M) Hash = H(M)
Chave simétrica compartilhada = K_i
|| = símbolo de concatenação

	Confidencialidade	Integridade	Autenticidade
1. A -> B: M || H(M)			
2. A -> B: M || E(K, H(M))			
3. A -> B: M || C(K, M)			
4. A -> B: E(K, M)			
5. A -> B: $E(K_2, M)$ || $C(K_1, E(K_2, M))$			

68. Desenhe os processos usando criptografia simétrica, hash e MAC de forma que os seguintes objetivos sejam atendidos na comunicação de mensagens entre Alice e Bob:

    a) Autenticação de mensagem enviada de Alice para Bob

    b) Autenticação e confidencialidade de mensagem enviada de Alice para Bob

69. Desenhe os processos usando somente criptografia simétrica, hash e/ou MAC, combinados de forma adequada (não é obrigatório o uso de todos) para que os seguintes objetivos sejam atendidos na comunicação de mensagens entre Alice e Bob: confidencialidade (sigilo), integridade e autenticidade da mensagem enviada de Alice para Bob.

70. Analise os itens (a), (b), (e), (f) da Figura 11.5 e da Tabela 11.3: Quais itens oferecem autenticação? Quais itens oferecem confidencialidade? Quais itens oferecem integridade da mensagem? Explique como cada item oferece autenticação e/ou confidencialidade.

71. Analise os itens (a), (b), (c) da Figura 11.4 e da Tabela 11.2: Quais itens oferecem autenticação? Quais itens oferecem confidencialidade? Quais itens oferecem integridade da mensagem? Explique como cada item oferece autenticação e/ou confidencialidade.

72. Consultado os seguintes documentos

    a) http://www.openwall.com/presentations/PHDays2014-Yescrypt/PHDays2014-Yescrypt.pdf

    b) http://www.openwall.com/presentations/Passwords12-The-Future-Of-Hashing/Passwords12-The-Future-Of-Hashing.pdf

    responda: quais são os métodos de derivação de chaves considerados mais fortes e mais fracos?

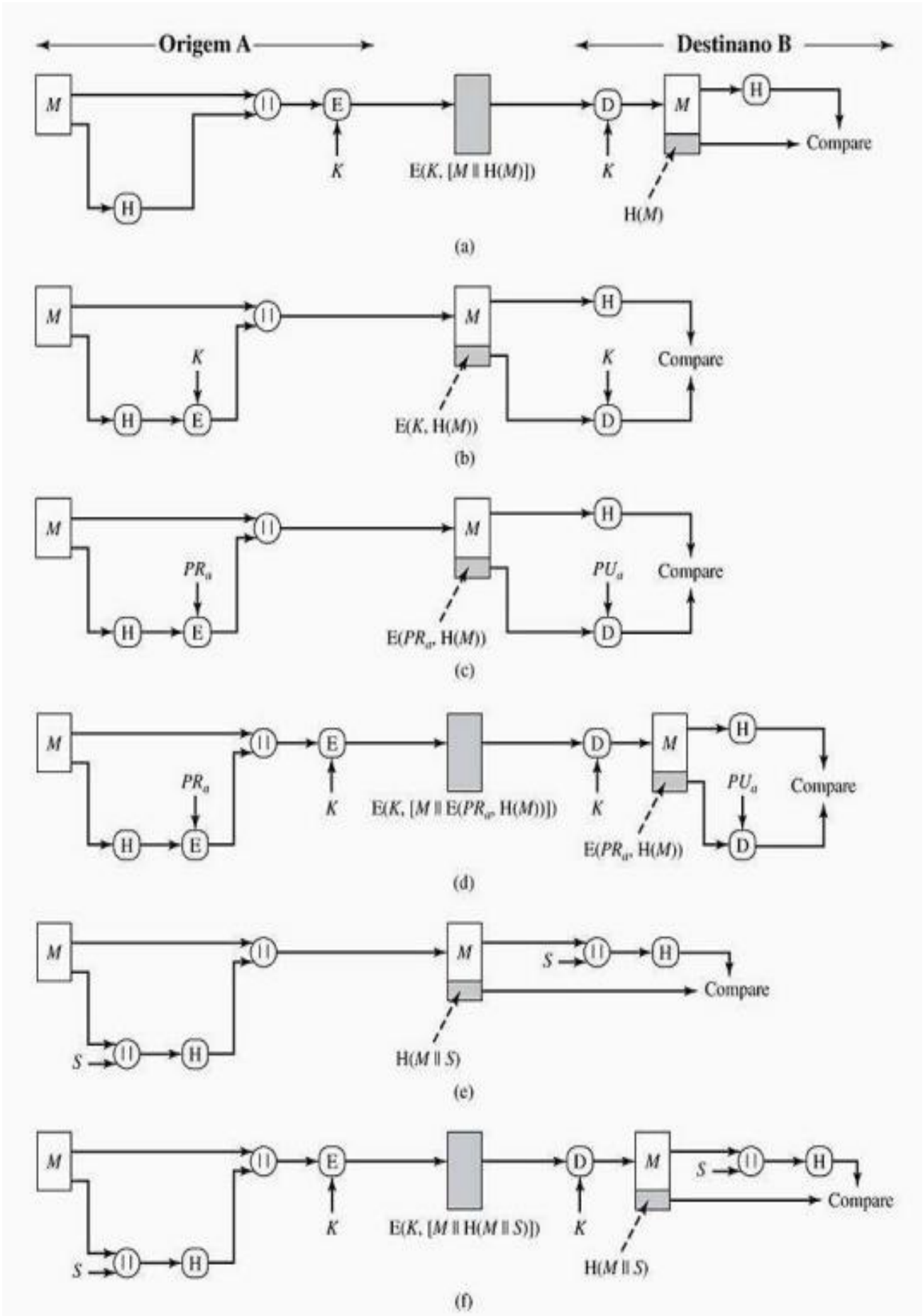


Figura 11.5 Usos básicos da função de hash.

Tabela 11.3 Usos básicos da função de hash H (ver Figura 11.5).

$A \rightarrow B: E(K, [M \| H(M)])$ • Oferece confidencialidade Somente A e B compartilham K • Oferece autenticação — $H(M)$ é protegido criptograficamente	$A \rightarrow B: E(K, [M \| E(PR_a, H(M))])$ • Oferece autenticação e assinatura digital • Oferece confidencialidade — Somente A e B compartilham K

(a) Criptografia de mensagem mais código de hash

(d) Criptografia do resultado de (c) — chave secreta compartilhada

$A \rightarrow B: M \| E(K, H(M))$ • Oferece autenticação — $H(M)$ é criptograficamente protegido	$A \rightarrow B: M \| H(M \| S)$ • Oferece autenticação — Somente A e B compartilham S

(b) Criptografia do código de hash — chave secreta compartilhada

(e) Cálculo do código de hash da mensagem mais o valor secreto

$A \rightarrow B: M \| E(PR_a, H(M))$ • Oferece autenticação e assinatura digital — $H(M)$ é criptograficamente protegido — Somente A poderia criar $E(PR_a, H(M))$	$A \rightarrow B: E(K, [M \| H(M \| S])$ • Oferece autenticação — Somente A e B compartilham S • Oferece confidencialidade — Somente A e B compartilham K

(c) Criptografia do código de hash — chave privada do emissor

(f) Encrypt result of (e)
Criptografia do resultado de (e)

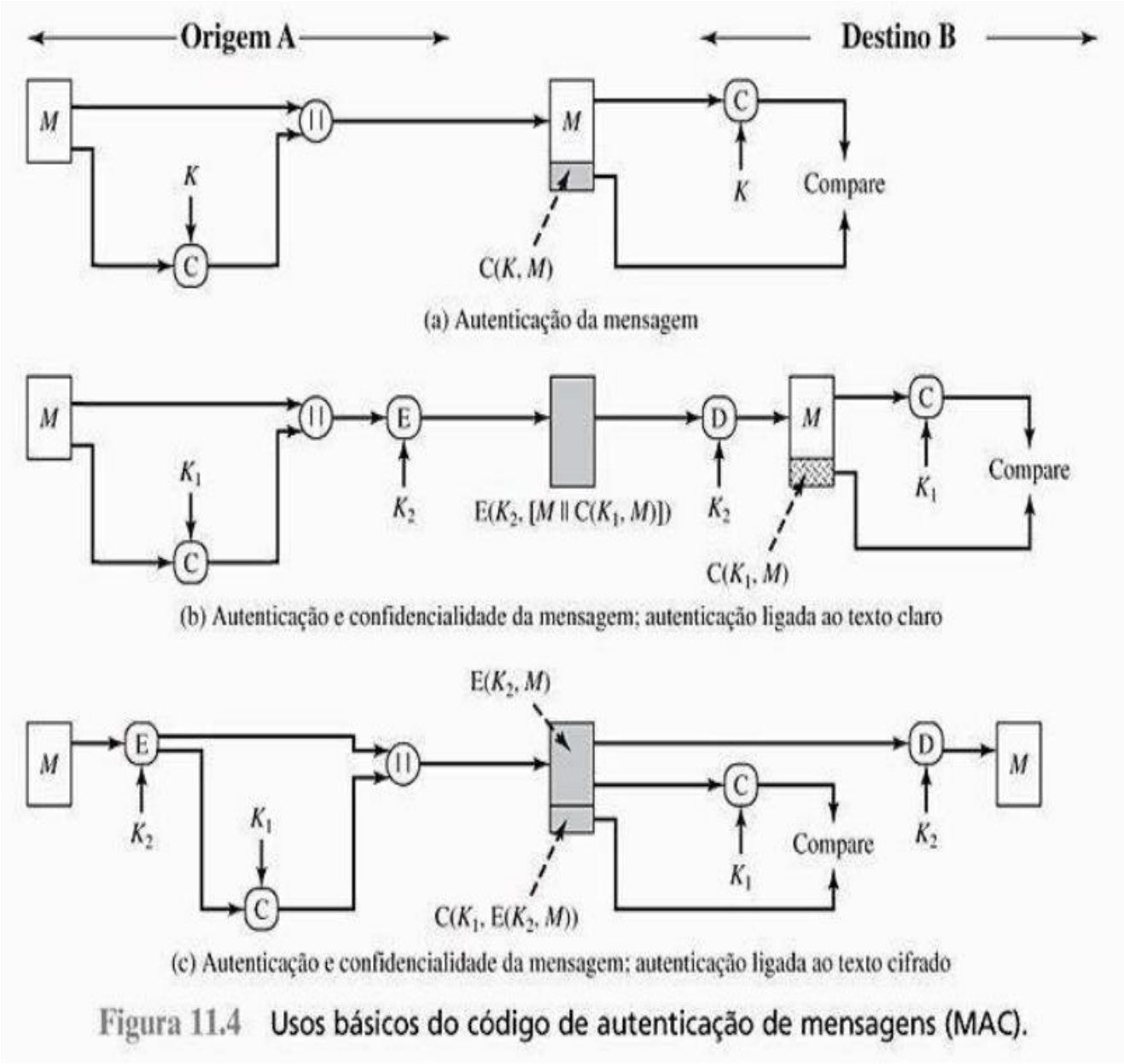


Figura 11.4 Usos básicos do código de autenticação de mensagens (MAC).

Tabela 11.2 Usos básicos do código de autenticação de mensagens C (ver Figura 11.4)

$A \rightarrow B: M \| C(K, M)$

- Oferece autenticação
  — Somente A e B compartilham K

(a) Autenticação da mensagem

$A \rightarrow B: E(K_2, [M \| C(K, M)])$

- Oferece autenticação
  — Somente A e B compartilham K_1
- Oferece confidencialidade
  — Somente A e B compartilham K_2

(b) Autenticação e confidencialidade da mensagem: autenticação ligada ao texto claro

$A \rightarrow B: E(K_2, M) \| C(K_1, E(K_2, M))$

- Oferece autenticação
  — Usando K_1
- Oferece confidencialidade
  — Usando K_2

(c) Autenticação e confidencialidade da mensagem: autenticação ligada ao texto cifrado