STUDENT

0027

TENTAMEN

2021-09-22 D0029E 0002

Kurskod	--
Bedömningsform	--
Starttid	22.09.2021 11:00
Sluttid	22.09.2021 14:30
Bedömningsfrist	--
PDF skapad	07.09.2022 12:15

Hash Functions

Fråga	Uppgiftstitel	Status	Poäng	Uppgiftstyp
ℹ	Hash Functions Main Questions			Dokument
1	Hash Functions 1	Delvis rätt	6/6	Textfält
2	Hash Functions 2	Obesvarad	0/10	Sifferfält
3	Hash Functions 3	Fel	10/10	Sifferfält
4	Hash Functions 4	Rätt	5/5	Flervalsfråga
☑	Hash Functions Notes	Obesvarad		Formulär

Secret Key

Fråga	Uppgiftstitel	Status	Poäng	Uppgiftstyp
5	Secret Key 1	Rätt	5/5	Sifferfält
6	Secret Key 2	Rätt	5/5	Flervalsfråga
7	Secret Key 3	Delvis rätt	0/16	Sifferfält
8	Secret Key 4	Fel	0/15	Flervalsfråga
☑	Secret Key Notes	Besvarad		Formulär

Public Key

Fråga	Uppgiftstitel	Status	Poäng	Uppgiftstyp
9	Public Key 1	Rätt	5/5	Sifferfält
10	Public Key 2	Fel	5/5	Sifferfält
11	Public Key 3	Rätt	15/15	Sifferfält
12	Public Key 4	Delvis rätt	12.5/15	Sifferfält
☑	Public Key Notes	Besvarad		Formulär

Multiple Choice Questions

Fråga	Uppgiftstitel	Status	Poäng	Uppgiftstyp
13	D0029E MCQ 9	Rätt	1/1	Flervalsfråga
14	D0029E MCQ 18	Fel	0/1	Flervalsfråga
15	D0029E MCQ 13	Rätt	1/1	Flervalsfråga
16	D0029E MCQ 2	Rätt	1/1	Flervalsfråga
17	D0029E MCQ 14	Rätt	1/1	Flervalsfråga
18	D0029E MCQ 5	Rätt	1/1	Flervalsfråga
19	D0029E MCQ 20	Rätt	1/1	Flervalsfråga
20	D0029E MCQ 8	Rätt	1/1	Flervalsfråga
21	D0029E MCQ 21	Fel	1/1	Flervalsfråga
22	D0029E MCQ 1	Rätt	1/1	Flervalsfråga
23	D0029E MCQ 19	Rätt	1/1	Flervalsfråga
24	D0029E MCQ 17	Rätt	1/1	Flervalsfråga
25	D0029E MCQ 25	Rätt	1/1	Flervalsfråga
26	D0029E MCQ 12	Rätt	1/1	Flervalsfråga
27	D0029E MCQ 23	Rätt	1/1	Flervalsfråga
28	D0029E MCQ 15	Rätt	1/1	Flervalsfråga
29	D0029E MCQ 24	Rätt	1/1	Flervalsfråga
30	D0029E MCQ 22	Rätt	1/1	Flervalsfråga
31	D0029E MCQ 3	Rätt	1/1	Flervalsfråga
32	D0029E MCQ 10	Rätt	1/1	Flervalsfråga

33	D0029E MCQ 4	Rätt	1/1	Flervalsfråga
34	D0029E MCQ 11	Rätt	1/1	Flervalsfråga
35	D0029E MCQ 16	Fel	0/1	Flervalsfråga

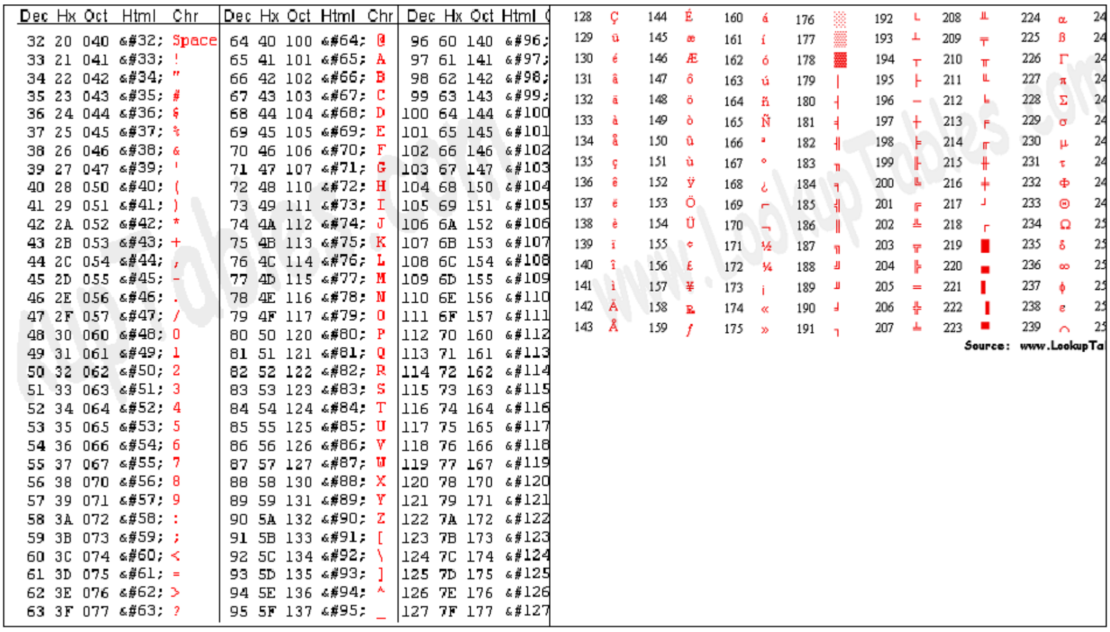
True and False

Fråga	Uppgiftstitel	Status	Poäng	Uppgiftstyp
36	D0029E TF 5	Rätt	1/1	Sant/Falskt
37	D0029E TF 6	Rätt	1/1	Sant/Falskt
38	D0029E TF 3	Rätt	1/1	Sant/Falskt
39	D0029E TF 4	Fel	0/1	Sant/Falskt
40	D0029E TF 12	Rätt	1/1	Sant/Falskt
41	D0029E TF 13	Rätt	1/1	Sant/Falskt
42	D0029E TF 1	Rätt	1/1	Sant/Falskt
43	D0029E TF 11	Rätt	1/1	Sant/Falskt
44	D0029E TF 9	Rätt	1/1	Sant/Falskt
45	D0029E TF 8	Rätt	1/1	Sant/Falskt
46	D0029E TF 14	Fel	0/1	Sant/Falskt
47	D0029E TF 7	Rätt	1/1	Sant/Falskt
48	D0029E TF 10	Rätt	1/1	Sant/Falskt
49	D0029E TF 2	Rätt	1/1	Sant/Falskt
50	D0029E TF 15	Rätt	1/1	Sant/Falskt

1 Hash Functions 1

Hash Functions 1) Using ASCII codes (the table is provided below, omit the white spaces) and the hash function defined above compute the digest of message in **decimal** form:

"JAG ÄR SKYLDIG DIG 10090 KR"



Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html C
32	20	040	&#32;	Space	64	40	100	&#64;	@	96	60	140	&#96;
33	21	041	&#33;	!	65	41	101	&#65;	A	97	61	141	&#97;
34	22	042	&#34;	"	66	42	102	&#66;	B	98	62	142	&#98;
35	23	043	&#35;	#	67	43	103	&#67;	C	99	63	143	&#99;
36	24	044	&#36;	$	68	44	104	&#68;	D	100	64	144	&#100
37	25	045	&#37;	%	69	45	105	&#69;	E	101	65	145	&#101
38	26	046	&#38;	&	70	46	106	&#70;	F	102	66	146	&#102
39	27	047	&#39;	'	71	47	107	&#71;	G	103	67	147	&#103
40	28	050	&#40;	(	72	48	110	&#72;	H	104	68	150	&#104
41	29	051	&#41;	)	73	49	111	&#73;	I	105	69	151	&#105
42	2A	052	&#42;	*	74	4A	112	&#74;	J	106	6A	152	&#106
43	2B	053	&#43;	+	75	4B	113	&#75;	K	107	6B	153	&#107
44	2C	054	&#44;	,	76	4C	114	&#76;	L	108	6C	154	&#108
45	2D	055	&#45;	-	77	4D	115	&#77;	M	109	6D	155	&#109
46	2E	056	&#46;	.	78	4E	116	&#78;	N	110	6E	156	&#110
47	2F	057	/	/	79	4F	117	&#79;	O	111	6F	157	&#111
48	30	060	&#48;	0	80	50	120	&#80;	P	112	70	160	&#112
49	31	061	&#49;	1	81	51	121	&#81;	Q	113	71	161	&#113
50	32	062	&#50;	2	82	52	122	R	R	114	72	162	&#114
51	33	063	&#51;	3	83	53	123	&#83;	S	115	73	163	&#115
52	34	064	&#52;	4	84	54	124	&#84;	T	116	74	164	&#116
53	35	065	&#53;	5	85	55	125	&#85;	U	117	75	165	&#117
54	36	066	&#54;	6	86	56	126	&#86;	V	118	76	166	&#118
55	37	067	&#55;	7	87	57	127	&#87;	W	119	77	167	&#119
56	38	070	&#56;	8	88	58	130	&#88;	X	120	78	170	&#120
57	39	071	&#57;	9	89	59	131	&#89;	Y	121	79	171	&#121
58	3A	072	&#58;	:	90	5A	132	&#90;	Z	122	7A	172	&#122
59	3B	073	&#59;	;	91	5B	133	&#91;	[	123	7B	173	&#123
60	3C	074	&#60;	<	92	5C	134	&#92;	\	124	7C	174	&#124
61	3D	075	&#61;	=	93	5D	135	&#93;	]	125	7D	175	&#125
62	3E	076	&#62;	>	94	5E	136	&#94;	^	126	7E	176	&#126
63	3F	077	&#63;	?	95	5F	137	&#95;	_	127	7F	177	&#127

128	Ç	144	É	160	á	176	░	192	└	208	╨	224	α	24
129	ü	145	æ	161	í	177	▒	193	┴	209	╤	225	ß	24
130	é	146	Æ	162	ó	178	▓	194	┬	210	╥	226	Γ	24
131	â	147	ô	163	ú	179	│	195	├	211	╙	227	π	24
132	ä	148	ö	164	ñ	180	┤	196	─	212	╘	228	Σ	24
133	à	149	ò	165	Ñ	181	╡	197	┼	213	╒	229	σ	24
134	å	150	û	166	ª	182	╢	198	╞	214	╓	230	µ	24
135	ç	151	ù	167	º	183	╖	199	╟	215	╫	231	τ	24
136	ê	152	ÿ	168	¿	184	╕	200	╚	216	╪	232	Φ	24
137	ë	153	Ö	169	⌐	185	╣	201	╔	217	┘	233	Θ	24
138	è	154	Ü	170	¬	186	║	202	╩	218	┌	234	Ω	25
139	ï	155	¢	171	½	187	╗	203	╦	219	█	235	δ	25
140	î	156	£	172	¼	188	╝	204	╠	220	▄	236	∞	25
141	ì	157	¥	173	¡	189	╜	205	═	221	▌	237	φ	25
142	Ä	158	₧	174	«	190	╛	206	╬	222	▐	238	ε	25
143	Å	159	ƒ	175	»	191	┐	207	╧	223	▀	239	∩	25

Source: www.LookupTa

ANSWER HERE (3 bytes per text entry under LETTERS column, decimal for each letter DECIMALS column)

LETTERS	DECIMALS(/result of mod 256 after each multiplications)		
JAG ✓	74 ✓	65 ✓	71 ✓
ÄRS ✓	142 ✓ / 12 ✓	82 ✓ / 210 ✓	83 ✓ / 5 ✓
KYL ✓	75 ✓ / 132 ✓	89 ✓ / 2 ✓	76 ✓ / 124 ✓
DIG ✓	68 ✓ / 16 ✓	73 ✓ / 146 ✓	71 ✓ / 100 ✓
DIG ✓	68 ✓ / 64 ✓	73 ✓ / 162 ✓	71 ✓ / 188 ✓
100 ✓	49 ✓ / 64 ✓	48 ✓ / 96 ✓	48 ✓ / 64 ✓
90K ✗ (95K)	57 ✓ / 64 ✓	48 ✗ (53) / 0 ✗ (224)	75 ✓ / 192 ✓
R ✗ (R11)	82 ✓ / 128 ✓	1 ✓	1 ✓
RESULT	000 ✗ (128)	000 ✗ (224)	000 ✗ (192)

Totalpoäng: 6

2 Hash Functions 2

Hash Functions 2) Construct the message authentication code using the following rule: MAC= H(K|m), where K is the shared secret

□ ✖ (128) □ ✖ (160) □ ✖ (192)

Put final answer above, show the working for this in the last question of this section on Hash Functions.

Totalpoäng: 10

3 Hash Functions 3

Hash Functions 3) In the meantime Joel and Kalle made a break and Joel decided to make Kalle to pay back more than he actually owes him. Can he do that by modifying the debt letter and still complying with the integrity check? Give an example that maximizes benefit to Joel.

Answer: Changing the amount to 80090 ✖ (95010) does not change MAC

Totalpoäng: 10

4 Hash Functions 4

Hash Functions 4) Which property(ies) should a hash function satisfy to prevent this scenario from happening?

Select one alternative:

○ They should produce at least 600 bit output

○ Should be possible to compute the original message from the output

● They are “collision-free.” ✓

○ They should produce different outputs for same input

Totalpoäng: 5

☑ Hash Functions Notes

Notes for Hash Functions 2

5 Secret Key 1

Consider a four-bit block cipher in the table below. Suppose the plaintext is 100110011001.

	Input Block	Output Block
1	0000	1001
2	0001	0010
3	0010	1110
4	0011	0100
5	0100	0000
6	0101	0111
7	0110	0001
8	0111	0011
9	1000	0101
10	1001	1101
11	1010	0110
12	1011	1010
13	1100	1111
14	1101	1011
15	1110	1100
16	1111	1000

Secret Key 1: Encrypt the plaintext using the given cipher in the ECB encryption mode. Write the resulting cipher text.

Answer: The cipher is 1101 ✓ 1101 ✓ 1101 ✓

Totalpoäng: 5

6 Secret Key 2

Secret Key 2: Suppose an attacker who does not know the cipher intercepts the encrypted message produced in the previous question (**Secret Key 1**). What can he or she deduce from it?

Select one alternative:

○ The first 4 bits is most likely an initialization vector (IV).

● That the plaintext message has a repeating pattern. ✓

○ Cannot deduce anything, it is heavily encrypted.

○ Number of 0’s is equal to number of 1’s.

Totalpoäng: 5

7 Secret Key 3

Secret Key 3: Encrypt the plaintext now using the 2-bit CFB mode. For this assume that IV is initialized as 1010. Present intermediate steps and the resulting ciphertext.

Answer: The cipher is 1 ✗ (1111) 0 ✓ 1101 ✗ (1010)

Show the working in the last question of this section

Totalpoäng: 16

8 Secret Key 4

Secret Key 4: Present a solution providing both message confidentiality and message integrity using the approach in step **Secret Key 3 question** as a base

Select one alternative:

○ One can do it with a same initialization vector IV.

○ Use CFB encryption with IV1 to produce cyphertext, Use the last cipherblock CFB encryption with IV2 as a message digest. ✓

○ This is impossible to do with CFB.

● Randomly choose IV for each encrypted block. ✗

Totalpoäng: 15

☑ Secret Key Notes

Show here the working for Secret Key 3 Question.

My answer on question secret key 3 changes everytime so I write my answer here aswell..

MY ANSWER: 0001 0000 1101

I got this by putting the IV (1010) into the block cipher encryption giving me 0110. This is XOR:ed with the first block of 2 bits giving

0110 XOR 10 = 0100 (I then use this as input for BCE giving me the output 0000)

0000 XOR 01 = 0001 --> 0010

0010 XOR 10 = 0000 --> 1001

1001 XOR 01 = 1000 --> 0101

0101 XOR 10 = 0011 --> 0100

0100 XOR 01 = 0101

Giving us 0001 0000 1101

9 Public Key 1

Linda want to sign electronically a message, which has digest (in hex) “0x00 0x00 0x00 0x09” using RSA algorithm. She chooses p=11, q=23.

Pubic Key 1: What are n and *φ(n)*?

Answer: N = 253 ✓ and phi = 220 ✓

Show the working in the last question of this section

Totalpoäng: 5

10 Public Key 2

Pubic Key 2: She has a choice of selecting **e** parameter to be either 20 or 17. Which one should she choose?

Answer: She chooses 1 ✗ (17) as the GCD of phi and e must be 17 ✗ (1)

Write the motivation for your answer in the last question of this section.

Totalpoäng: 5

11 Public Key 3

Pubic Key 3: Using Euclid’s algorithm find **d**, which is multiplicative inverse to e (*mod φ(n)*).

Answer: d = 13 ✓

Show all steps for your answer in the last question of this section.

Totalpoäng: 15

12 Public Key 4

Pubic Key 4: Write the resulting private and the public keys. Encrypt the digest of Linda's message using the appropriate key. Show that it works by decrypting the message.

Answer: Private key = (13 ✓ , 253 ✓), Public Key = (17 ✓ , 253 ✓)

CT = 26 ✗ (58)

PT = 9 ✓

Show calculation in the last question of this section.

Totalpoäng: 15

☑ Public Key Notes

Show notes/working for Public Key 1

n = p*q = 11 * 23 = 253

phi(n) = phi(11) * phi(23) = (11 - 1) * (23 - 1) = 220

Show notes/working for Public Key 2

gcd(220, 20) = 11 so that does not work

gcd(220, 17) = 1 <-- perfect

Show notes/working for Public Key 3

17 * d mod 220 = 1 <=>

17 * d + 220 * y = 1, (try with y = -1) <=>

17 * d - 220 = 1 <=>

d = 221 / 17 = 13

Show notes/working for Public Key 4

CT:

9^17 mod 253 = 26 (Dec)

PT:

26^13 mod 253 = 9 (Dec)

13 D0029E MCQ 9

On average, ________________ of all possible keys must be tried in order to achieve success with a brute-force attack.

Select one alternative:

○ One-Fourth

○ Three-Fourths

● Half ✓

○ Two-Thirds

Totalpoäng: 1

14 D0029E MCQ 18

The exact substitutions and transformations performed by the algorithm depend on the

____

Select one alternative:

○ Ecnryption Algorithm

○ Secret Key ✓

○ Decryption Algorithm

● Plaintext ✗

Totalpoäng: 1

15 D0029E MCQ 13

________________ is the granting of a right or permission to a system entity to access a system resource.

Select one alternative:

● Authorization ✓

○ Monitoring

○ Authentication

○ Control

Totalpoäng: 1

16 D0029E MCQ 2

________________ assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

Select one alternative:

● System Integrity ✓

○ Data Integrity

○ Availability

○ Confidentiality

Totalpoäng: 1

17 D0029E MCQ 14

________________ is the traditional method of implementing access control.

Select one alternative:

○ MBAC

● DAC ✓

○ MAC

○ RBAC

Totalpoäng: 1

18 D0029E MCQ 5

A flaw or weakness in a system’s design, implementation, or operation and management that could be exploited to violate the system’s security policy is ______________.

Select one alternative:

○ Adversary

○ Countermeasure

○ Risk

● Vulnerability ✓

Totalpoäng: 1

19 D0029E MCQ 20

If the analyst is able to get the source system to insert into the system a message chosen by the analyst, then a _____________ attack is possible.

Select one alternative:

○ Know IV

○ Chosen Ciphertext

● Chosen Plaintext ✓

○ Known Plaintext

Totalpoäng: 1

20 D0029E MCQ 8

The ________________ is the scrambled message produced as output.

Select one alternative:

○ Cryptanalysis

○ Plain Text

● Cipher Text ✓

○ Secret Key

Totalpoäng: 1

21 D0029E MCQ 21

The most widely used encryption scheme is based on the _____________ adopted in 1977 by the National Bureau of Standards.

Select one alternative:

○ 3DES

○ CES

○ AES ✓

● DES ✗

Totalpoäng: 1

22 D0029E MCQ 1

_________________ assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

Select one alternative:

○ Data Integrity

○ System Integrity

○ Availability

● Privacy ✓

Totalpoäng: 1

23 D0029E MCQ 19

The ______________ is the encryption algorithm run in reverse.

Select one alternative:

○ Ecnryption Algorithm

○ Plaintext

● Decryption Algorithm ✓

○ Secret Key

Totalpoäng: 1

24 D0029E MCQ 17

_________________ is the original message or data that is fed into the algorithm as input.

Select one alternative:

○ Encryption Algorithm

○ Decryption Algorithm

○ Ciphertext

● Plaintext ✓

Totalpoäng: 1

25 D0029E MCQ 25

A ___________ attack involves trying all possible private keys.

Select one alternative:

- ● Brute Force ✓
- ○ Timing
- ○ Mathematical
- ○ Chosen Ciphertext

Totalpoäng: 1

26 D0029E MCQ 12

_________________ is verification that the credentials of a user or other system entity are valid.

Select one alternative:

- ○ Adequacy
- ● Authentication ✓
- ○ Authorization
- ○ Audit

Totalpoäng: 1

27 D0029E MCQ 23

In 2005, NIST announced the intention to phase out approval of _____________ and move to a reliance on the other SHA versions by 2010.

Select one alternative:

○ SHA-512

○ SHA-2

○ SHA-256

● SHA-1 ✓

Totalpoäng: 1

28 D0029E MCQ 15

_________________ are either individuals or members of a larger group of outsider attackers who are motivated by social or political causes.

Select one alternative:

○ Others

● Activists ✓

○ Cyber criminals

○ State-sponsored organizations

Totalpoäng: 1

29 D0029E MCQ 24

The _____________ scheme has reigned supreme as the most widely accepted and implemented approach to public-key encryption.

Select one alternative:

○ HMAC

○ SHA-1

● RSA ✓

○ MD5

Totalpoäng: 1

30 D0029E MCQ 22

SHA-1 produces a hash value of ______________ bits.

Select one alternative:

○ 384

○ 180

● 160 ✓

○ 256

Totalpoäng: 1

31

D0029E MCQ 3

A loss of ___________ is the unauthorized disclosure of information.

Select one alternative:

○ Authenticity

● Confidentiality ✓

○ Availability

○ Integrity

Totalpoäng: 1

32

D0029E MCQ 10

The most important symmetric algorithms, all of which are block ciphers, are the DES, triple DES, and the _________________.

Select one alternative:

○ DSS

○ SHA

● AES ✓

○ RSA

Totalpoäng: 1

33 D0029E MCQ 4

A ______________ level breach of security could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

Select one alternative:

○ Moderate

○ Low

● High ✓

○ Normal

Totalpoäng: 1

34 D0029E MCQ 11

________________ implements a security policy that specifies who or what may have access to each specific system resource and the type of access that is permitted in each instance.

Select one alternative:

● Access control ✓

○ System control

○ Audit control

○ Resource control

Totalpoäng: 1

35 D0029E MCQ 16

________________ is a security event that constitutes a security incident in which an intruder gains access to a system without having authorization to do so.

Select one alternative:

○ IDS

● Intrusion Detection ✗

○ Criminal Enterprise

○ Security Intrusion ✓

Totalpoäng: 1

36 D0029E TF 5

Triple DES takes a plaintext block of 64 bits and a key of 56 bits to produce a ciphertext block of 64 bits.

Select one alternative:

● False ✓

○ True

Totalpoäng: 1

37 D0029E TF 6

Symmetric encryption is also referred to as secret-key or single-key encryption.

Select one alternative:

○ False

● True ✓

Totalpoäng: 1

38 D0029E TF 3

Cryptanalytic attacks try every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained.

Select one alternative:

● False ✓

○ True

Totalpoäng: 1

39 D0029E TF 4

The secret key is input to the encryption algorithm.

Select one alternative:

○ True ✓

● False ✗

Totalpoäng: 1

40 D0029E TF 12

SHA is perhaps the most widely used family of hash functions.

Select one alternative:

● True ✓

○ False

Totalpoäng: 1

41 D0029E TF 13

SHA-1 is considered to be very secure.

Select one alternative:

● False ✓

○ True

Totalpoäng: 1

42 D0029E TF 1

Symmetric encryption is used primarily to provide confidentiality.

Select one alternative:

○ False

● True ✓

Totalpoäng: 1

43 D0029E TF 11

The one-way hash function is important not only in message authentication but also in digital signatures.

Select one alternative:

● True ✓

○ False

Totalpoäng: 1

44 D0029E TF 9

The ciphertext-only attack is the easiest to defend against.

Select one alternative:

○ False

● True ✓

Totalpoäng: 1

45 D0029E TF 8

If both sender and receiver use the same key the system is referred to as asymmetric.

Select one alternative:

○ True

● False ✓

Totalpoäng: 1

46 D0029E TF 14

SHA-2 shares the same structure and mathematical operations as its predecessors and this is a cause for concern.

Select one alternative:

● False ✗

○ True ✓

Totalpoäng: 1

47 D0029E TF 7

Plaintext is the scrambled message produced as output.

Select one alternative:

● False ✓

○ True

Totalpoäng: 1

48 D0029E TF 10

A brute-force approach involves trying every possible key until an intelligible translation of the ciphertext into plaintext is obtained.

Select one alternative:

● True ✓

○ False

Totalpoäng: 1

49 D0029E TF 2

Two of the most important applications of public-key encryption are digital signatures and key management.

Select one alternative:

● True ✓

○ False

Totalpoäng: 1

50 D0029E TF 15

HMAC can be proven secure provided that the embedded hash function has some reasonable cryptographic strengths.

Select one alternative:

● True ✓

○ False

Totalpoäng: 1