Question **1**

Answer saved

Marked out of 1.00

Цезар шифрлэл key=3, text="krypto"

Select one:

- a. crypto
- b. yptokr
- c. fubswr
- d. ryptok

Clear my choice

Question **2**

Answer saved

Marked out of 1.00

Аль нь cipher вэ?

Select one:

- a. энгийн текстийг шифрлэсэн текстэд хөрвүүлэх алгоритм
- b. илгээгч болон хүлээн авагч мэдээллийг тайлхад хэрэглэдэг түлхүүр
- c. энгийн текст
- d. шифрлэсэн текст

Clear my choice

Question **3**

Answer saved

Marked out of 1.00

Цезар шифрлэл key=3, text="fubswr"

Select one:

- a. crypto
- b. jyfwav
- c. hwduyt
- d. fubswh

Clear my choice

◄ Лаб 1, 2 шифрлэх файл

Question **4**

Answer saved

Marked out of 1.00

Аль нь ciphertext вэ?

Select one:

- a. шифрлэсэн текст
- b. энгийн текст
- c. энгийн текстийг шифрлэсэн текстэд хөрвүүлэх алгоритм
- d. илгээгч болон хүлээн авагч мэдээллийг тайлхад хэрэглэдэг түлхүүр

Clear my choice

Question **5**

Answer saved

Marked out of 1.00

Цезар шифрлэл key=7, text="jyfwav"

Select one:

- a. hwduyt
- b. crypto
- c. fubswr
- d. jyfwav

Clear my choice

Question **6**

Answer saved

Marked out of 1.00

Аль нь key вэ?

Select one:

- a. энгийн текстийг шифрлэсэн текстэд хөрвүүлэх алгоритм
- b. илгээгч болон хүлээн авагч мэдээллийг тайлхад хэрэглэдэг түлхүүр
- c. энгийн текст
- d. шифрлэсэн текст

Clear my choice

◄ Лаб 1, 2 шифрлэх файл

Question **10**

Answer saved

Marked out of 1.00

Аль нь encrypt вэ?

Select one:

- a. шифрлэсэн текстийг энгийн текстэд хөрвүүлэх
- b. шифер тайлах арга ухаан судлана
- c. энгийн текстийг шифрлэсэн текстэд хөрвүүлэх
- d. шифрлэх арга ухаанд суралцах

Clear my choice

Question **11**

Answer saved

Marked out of 1.00

Аль нь cryptanalysis вэ?

Select one:

- a. энгийн текстийг шифрлэсэн текстэд хөрвүүлэх
- b. шифрлэсэн текстийг энгийн текстэд хөрвүүлэх
- c. шифер тайлах арга ухаан судлана
- d. шифрлэх арга ухаанд суралцах

Clear my choice

Question **12**

Answer saved

Marked out of 1.00

Аль нь plaintext вэ?

Select one:

- a. илгээгч болон хүлээн авагч мэдээллийг тайлхад хэрэглэдэг түлхүүр
- b. шифрлэсэн текст
- c. энгийн текстийг шифрлэсэн текстэд хөрвүүлэх алгоритм
- d. энгийн текст

Clear my choice

◄ Лаб 1, 2 шифрлэх файл

Question **7**

Answer saved

Marked out of 1.00

Аль нь cryptography вэ?

Select one:

- a. шифрлэх арга ухаанд суралцах
- b. шифрлэсэн текстийг энгийн текстэд хөрвүүлэх
- c. шифер тайлах арга ухаан судлана
- d. энгийн текстийг шифрлэсэн текстэд хөрвүүлэх

Clear my choice

Question **8**

Answer saved

Marked out of 1.00

Цезар шифрлэл key=5, text="crypto"

Select one:

- a. fubswr
- b. hwduyt
- c. yptokr
- d. krypto

Clear my choice

Question **9**

Answer saved

Marked out of 1.00

Цезар шифрлэл key=7, text="crypto"

Select one:

- a. krypto
- b. jyfwav
- c. hwduyt
- d. fubswr

Clear my choice

◄ Лаб 1, 2 шифрлэх файл

Question **13**

Answer saved

Marked out of 1.00

Аль нь decrypt вэ?

Select one:

- a. шифер тайлах арга ухаан судлана
- b. шифрлэх арга ухаанд суралцах
- c. энгийн текстийг шифрлэсэн текстэд хөрвүүлэх
- d. шифрлэсэн текстийг энгийн текстэд хөрвүүлэх

Clear my choice

◄ Лаб 1, 2 шифрлэх файл

Jump to...

Лекц 2 ►

Started on	Sunday, 20 February 2022, 3:41 PM
State	Finished
Completed on	Sunday, 20 February 2022, 3:45 PM
Time taken	3 mins 56 secs
Grade	**5.00** out of 5.00 (**100**%)

Question **1**

Correct

Mark 1.00 out of 1.00

playfair шифрлэлт GRAVITYFLSBCDEHKMNOPQUWXZ Text="Kripto"

Select one:

- a. GFFGMB
- b. KRIPTO
- c. AGKSPM
- d. MGSZLK ✔

The correct answer is: MGSZLK

Question **2**

Correct

Mark 1.00 out of 1.00

playfair шифрлэлт GRAVITYFLSBCDEHKMNOPQUWXZ Text="Newspaper"

Select one:

- a. ODZFINVWIN
- b. ODZFNIINOV
- c. NEWSPAPER
- d. ODZFNIOHVU ✔

The correct answer is: ODZFNIOHVU

Question **3**

Correct

Mark 1.00 out of 1.00

playfair шифрлэлт GRAVITYFLSBCDEHKMNOPQUWXZ Text="Attack"

Select one:

- a. GFFGBM ✔
- b. GFGFMB
- c. GFFGMB
- d. ATTACK

The correct answer is: GFFGBM

Question **4**

Correct

Mark 1.00 out of 1.00

Vigenère шифрлэлт Text="apple", key="cryptii"

Select one:

- a. apple
- b. crnpi
- c. cgyee
- d. cgnax ✔

The correct answer is: cgnax

Question **5**

Correct

Mark 1.00 out of 1.00

Vigenère шифрлэлт Text="quick", key="cryptii"

Select one:

- a. slaxd
- b. slgrd ✔
- c. quick
- d. wtgzt

The correct answer is: slgrd

◄ лабораторын заавар 2

Jump to...

Question **1**

Answer saved

Marked out of 1.00

Аль нь 01001111-н swap вэ?

Select one:

- a. 00110100
- b. 00000101
- c. 11010100
- d. 11110100

Clear my choice

Question **2**

Answer saved

Marked out of 1.00

Аль нь 79-н битүүд вэ?

Select one:

- a. 01000011
- b. 01001101
- c. 01010000
- d. 01001111

Clear my choice

Question **3**

Answer saved

Marked out of 1.00

Аль нь 11010100 XOR 01001101 вэ?

Select one:

- a. 01110111
- b. 01010101
- c. 10011001
- d. 10111011

Clear my choice

◄ Зарлал

Question **4**

Answer saved

Marked out of 1.00

Аль нь 01010101-н 2 бит round shift вэ?

Select one:

- a. 01100110
- b. 01010101
- c. 11101110
- d. 11011101

Clear my choice

Question **5**

Answer saved

Marked out of 1.00

Аль нь 10111011-н 2 бит round shift вэ?

Select one:

- a. 01010101 01010101
- b. 01100110 10011001
- c. 11011101
- d. 11101110

Clear my choice

Question **6**

Answer saved

Marked out of 1.00

Аль нь 67-н битүүд вэ?

Select one:

- a. 01001111
- b. 01000011
- c. 01010000
- d. 01001101

Clear my choice

◄ Зарлал

Question **7**

Answer saved

Marked out of 1.00

Аль нь E-үсгийн битүүд вэ?

Select one:

- a. 01010100
- b. 01010000
- c. 01000101
- d. 01010101

Clear my choice

Question **8**

Answer saved

Marked out of 1.00

Аль нь 80-н битүүд вэ?

Select one:

- a. 01001111
- b. 01000011
- c. 01010000
- d. 01001101

Clear my choice

Question **9**

Answer saved

Marked out of 1.00

Аль нь 00000101 XOR 01010000 вэ?

Select one:

- a. 01010101
- b. 01110111
- c. 10011001
- d. 10111011

Clear my choice

◄ Зарлал

Question **10**

Answer saved

Marked out of 1.00

Аль нь U-үсгийн битүүд вэ?

Select one:

- a. 01010000
- b. 01000101
- c. 01010101
- d. 01010100

Clear my choice

Question **11**

Answer saved

Marked out of 1.00

Аль нь 01010000-н swap вэ?

Select one:

- a. 00110100
- b. 00000101
- c. 11010100
- d. 11110100

Clear my choice

Question **12**

Answer saved

Marked out of 1.00

Аль нь 11110100 XOR 01001111 вэ?

Select one:

- a. 10011001
- b. 01010101
- c. 01110111
- d. 10111011

Clear my choice

◄ Зарлал

Question **13**

Answer saved

Marked out of 1.00

Аль нь 77-н битүүд вэ?

Select one:

- a. 01001111
- b. 01001101
- c. 01000011
- d. 01010000

Clear my choice

Question **14**

Answer saved

Marked out of 1.00

Аль нь 01001101-н swap вэ?

Select one:

- a. 11110100
- b. 11010100
- c. 00110100
- d. 00000101

Clear my choice

Question **15**

Answer saved

Marked out of 1.00

Аль нь T-үсгийн битүүд вэ?

Select one:

- a. 01000101
- b. 01010100
- c. 01010000
- d. 01010101

Clear my choice

◄ Зарлал

Question **16**

Answer saved

Marked out of 1.00

Аль нь 00110100 XOR 01000011 вэ?

Select one:

- a. 01010101
- b. 10011001
- c. 10111011
- d. 01110111

Clear my choice

Question **17**

Answer saved

Marked out of 1.00

Аль нь 01000011-н swap вэ?

Select one:

- a. 11010100
- b. 00000101
- c. 00110100
- d. 11110100

Clear my choice

Question **18**

Answer saved

Marked out of 1.00

Аль нь 01110111-н 2 бит round shift вэ?

Select one:

- a. 01010101 01010101
- b. 11101110 10111011
- c. 01100110 10011001
- d. 11011101

Clear my choice

◄ Зарлал

Question **19**

Answer saved

Marked out of 1.00

Аль нь P-үсгийн битүүд вэ?

Select one:

- a. 01010101
- b. 01000101
- c. 01010000
- d. 01010100

Clear my choice

Question **20**

Answer saved

Marked out of 1.00

Аль нь 10011001-н 2 бит round shift вэ?

Select one:

- a. 01100110
- b. 11101110
- c. 01010101 01010101
- d. 11011101

Clear my choice

◄ Зарлал

Jump to...

Шалгалт 1-3 лекцийн хүрээнд ►

Question **1**

Not yet answered

Marked out of 16.00

Зураг дээр S-Box - н утгыг байрлуул. SubBytes transformation use S-Box

x \ y	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	52	09	6A	D5	04	26	A5	38	BF	40	A3	9E	81	F3	D7	FB
1	7C	E3	39	82	9B	2F	FF	87	34	8E	43	44	C4	DE	E9	CB
2	54	7B	94	32	A6	C2	23	3D	EE	4C	95	0B	42	FA	C3	4E
3	08	2E	A1	66	28	D9	24	B2	76	5B	A2	49	6D	8B	D1	25
4	72	F8	F6	64	86	68	98	16	D4	A4	5C	CC	5D	65	B6	92
5	6C	70	48	50	FD	ED	B9	DA	5E	15	46	57	A7	8D	9D	84
6	90	D8	AB	00	8C	BC	D3	0A	F7	E4	58	05	B8	B3	45	06
7	D0	2C	1E	8F	CA	3F	0F	02	C1	AF	BD	03	01	13	8A	6B
8	3A	91	11	41	4F	67	DC	EA	97	F2	CF	CE	F0	B4	E6	73
9	96	AC	74	22	E7	AD	35	85	E2	F9	37	E8	1C	75	DF	6E
A	47	F1	1A	71	1D	29	C5	89	6F	B7	62	0E	AA	18	BE	1B
B	FC	56	3E	4B	C6	D2	79	20	9A	DB	C0	FE	78	CD	5A	F4
C	1F	DD	A8	33	88	07	C7	31	B1	12	10	59	27	80	EC	5F
D	60	51	7F	A9	19	B5	4A	0D	2D	E5	7A	9F	93	C9	9C	EF
E	A0	E0	3B	4D	AE	2A	F5	B0	C8	EB	BB	3C	83	53	99	61
F	17	2B	04	7E	BA	77	D6	26	E1	69	14	63	55	21	0C	7D

98 04 5C EA AD 2D 45 96 33 83 F0 B0 85 C5 65 5D

Question **2**

Not yet answered

Marked out of 1.00

AES Багана холих '*' бит шилжүүлэх, 'x'=XOR, MixColumn s= F2 x (2 * 4C) x (3 * E7) x 8C

Select one:

- a. s=A5
- b. s=D4
- c. s=E4
- d. s=40

Clear my choice

Question **3**

Not yet answered

Marked out of 1.00

AES Багана холих '*' бит шилжүүлэх, 'x'=XOR, MixColumn s= (2 * F2) x (3 * 4C) x E7 x 8C

Select one:

- a. s=E4
- b. s=40
- c. s=D4
- d. s=A5

Clear my choice

Question **4**

Not yet answered

Marked out of 1.00

AES Мөр хувиргалт (ShiftRows)
AC EF 13 45
73 C1 B5 23
CF 11 D6 5A
7B DF B5 B8

AC EF 13 45	1-р мөр
D6 5A CF 11	3-р мөр
C1 B5 23 73	2-р мөр
B8 7B DF B5	4-р мөр

Question **5**

Not yet answered

Marked out of 1.00

AES Мөр хувиргалт (ShiftRows)
52 85 E3 F6
50 A4 11 CF
2F 5E C8 6A
28 D7 07 94

94 28 D7 07	4-р мөр
C8 6A 2F 5E	3-р мөр
52 85 E3 F6	1-р мөр
A4 11 CF 50	2-р мөр

Question **1**

Answer saved

Marked out of 1.00

AES Багана холих '*' бит шилжүүлэх, 'x'=XOR, MixColumn s=F2 x 4C x (2 * E7) x (3 * 8C)

Select one:

- a. s=D4
- b. s=A5
- c. s=E4
- d. s=40

Clear my choice

Question **2**

Not yet answered

Marked out of 1.00

AES Багана холих '*' бит шилжүүлэх, 'x'=XOR, MixColumn s= F2 x (2 * 4C) x (3 * E7) x 8C

Select one:

- a. s=A5
- b. s=D4
- c. s=40
- d. s=E4

Clear my choice

Question **3**

Answer saved

Marked out of 1.00

AES Мөр хувиргалт (ShiftRows)
87 F2 4D 97
EC 6E 4C 90
4A C3 46 E7
8C D8 95 A6

6E 4C 90 EC	2-р мөр
A6 8C D8 95	4-р мөр
46 E7 4A C3	3-р мөр
87 F2 4D 97	1-р мөр

Question **4**

Answer saved

Marked out of 4.00

AES Багана холих '*' бит шилжүүлэх, 'x'=XOR, MixColumn

s= (2 * 97) x (3 * EC) x C3 x 95 = 4C

s= 97 x (2 * EC) x (3 * C3) x 95 = 9F

s=97 x EC x (2 * C3) x (3 * 95) = 42

s=(3 * 97) x EC x C3 x (2 * 95) = BC

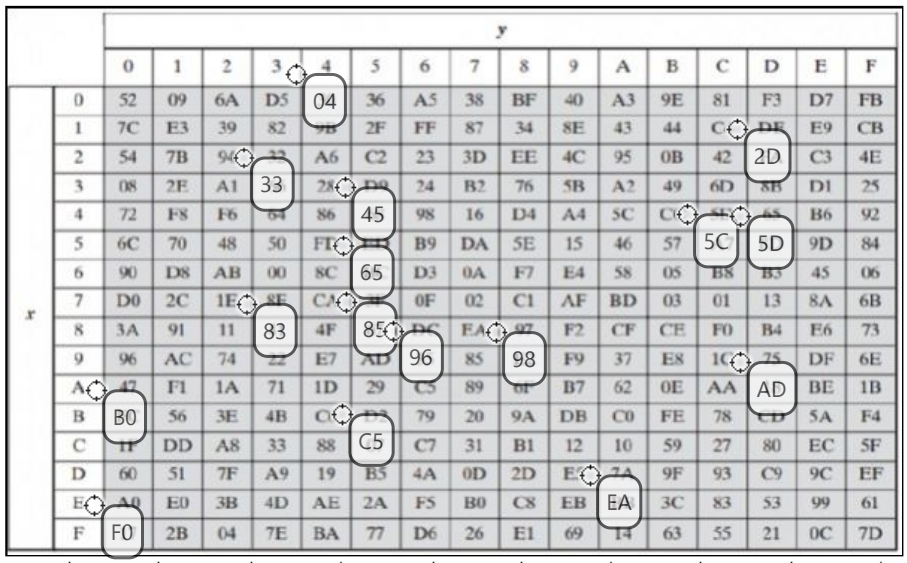
4B 9E

Question **5**

Not yet answered

Marked out of 16.00

Зураг дээр S-Box - н утгыг байрлуул. SubBytes transformation use S-Box



x \ y	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	52	09	6A	D5	04	36	A5	38	BF	40	A3	9E	81	F3	D7	FB
1	7C	E3	39	82	9B	2F	FF	87	34	8E	43	44	C4	DE	E9	CB
2	54	7B	94	32	A6	C2	23	3D	EE	4C	95	0B	42	2D	C3	4E
3	08	2E	A1	33	28	D9	24	B2	76	5B	A2	49	6D	8B	D1	25
4	72	F8	F6	64	86	45	98	16	D4	A4	5C	CC	5D	65	B6	92
5	6C	70	48	50	FD	ED	B9	DA	5E	15	46	57	5C	5D	9D	84
6	90	D8	AB	00	8C	65	D3	0A	F7	E4	58	05	B8	B3	45	06
7	D0	2C	1E	8F	CA	3F	0F	02	C1	AF	BD	03	01	13	8A	6B
8	3A	91	11	83	4F	85	DC	EA	97	F2	CF	CE	F0	B4	E6	73
9	96	AC	74	22	E7	AD	96	85	98	F9	37	E8	1C	75	DF	6E
A	47	F1	1A	71	1D	29	C5	89	6F	B7	62	0E	AA	AD	BE	1B
B	B0	56	3E	4B	C6	D2	79	20	9A	DB	C0	FE	78	CD	5A	F4
C	1F	DD	A8	33	88	C5	C7	31	B1	12	10	59	27	80	EC	5F
D	60	51	7F	A9	19	B5	4A	0D	2D	E5	7A	9F	93	C9	9C	EF
E	A0	E0	3B	4D	AE	2A	F5	B0	C8	EB	EA	3C	83	53	99	61
F	F0	2B	04	7E	BA	77	D6	26	E1	69	14	63	55	21	0C	7D

AD 83 5D 98 2D 33 5C F0 04 45 EA 65 B0 85 96 C5

◄ Даалгавар илгээх

Jump to...

Шалгалт 3-5-р лекцийн хүрээнд ►

Question **6**

Answer saved

Marked out of 4.00

AES Багана холих '*' бит шилжүүлэх, 'x'=XOR, MixColumn

s= (2 * 4D) x (3 * 90) x 4A x D8 = A3

s= 4D x (2 * 90) x (3 * 4A) x D8 = 70

s=4D x 90 x (2 * 4A) x (3 * D8) = 3A

s=(3 * 4D) x 90 x 4A x (2 * D8) = A6

Question **7**

Answer saved

Marked out of 1.00

AES Багана холих '*' бит шилжүүлэх, 'x'=XOR, MixColumn s=(3 * 87) x 6E x 46 x (2 * A6)

Select one:

- a. s=94
- b. s=37
- c. s=ED
- d. s=47

Clear my choice

Question **8**

Answer saved

Marked out of 1.00

AES Мөр хувиргалт (ShiftRows)
AC EF 13 45
73 C1 B5 23
CF 11 D6 5A
7B DF B5 B8

C1 B5 23 73	2-р мөр
D6 5A CF 11	3-р мөр
B8 7B DF B5	4-р мөр
AC EF 13 45	1-р мөр

Question **9**

Answer saved

Marked out of 1.00

AES Мөр хувиргалт (ShiftRows)
52 85 E3 F6
50 A4 11 CF
2F 5E C8 6A
28 D7 07 94

94 28 D7 07	4-р мөр
52 85 E3 F6	1-р мөр
A4 11 CF 50	2-р мөр
C8 6A 2F 5E	3-р мөр

Question **10**

Answer saved

Marked out of 1.00

AES Мөр хувиргалт (ShiftRows)
49 45 7F 77
DE DB 39 02
D2 96 87 53
89 F1 1A 3B

3B 89 F1 1A	4-р мөр
49 45 7F 77	1-р мөр
87 53 D2 96	3-р мөр
DB 39 02 DE	2-р мөр

◄ Даалгавар илгээх

Jump to...

Шалгалт 3-5-р лекцийн хүрээнд ►

Question **11**

Answer saved

Marked out of 1.00

AES Багана холих '*' бит шилжүүлэх, 'x'=XOR, MixColumn s= 87 x (2 * 6E) x (3 * 46) x A6

Select one:

- a. s=37
- b. s=94
- c. s=47
- d. s=ED

Clear my choice

Question **12**

Answer saved

Marked out of 1.00

AES Багана холих '*' бит шилжүүлэх, 'x'=XOR, MixColumn s= (2 * 87) x (3 * 6E) x 46 x A6

Select one:

- a. s=37
- b. s=94
- c. s=47
- d. s=ED

Clear my choice

Question **13**

Answer saved

Marked out of 1.00

AES Багана холих '*' бит шилжүүлэх, 'x'=XOR, MixColumn s= (2 * F2) x (3 * 4C) x E7 x 8C

Select one:

- a. s=D4
- b. s=E4
- c. s=40
- d. s=A5

Clear my choice

Question **14**

Answer saved

Marked out of 1.00

AES Багана холих '*' бит шилжүүлэх, 'x'=XOR, MixColumn s=87 x 6E x (2 * 46) x (3 * A6)

Select one:

- a. s=47
- b. s=94
- c. s=37
- d. s=ED

Clear my choice

Question **15**

Answer saved

Marked out of 1.00

AES Багана холих '*' бит шилжүүлэх, 'x'=XOR, MixColumn s=(3 * F2) x 4C x E7 x (2 * 8C)

Select one:

- a. s=40
- b. s=A5
- c. s=E4
- d. s=D4

Clear my choice

◄ Даалгавар илгээх

Jump to...

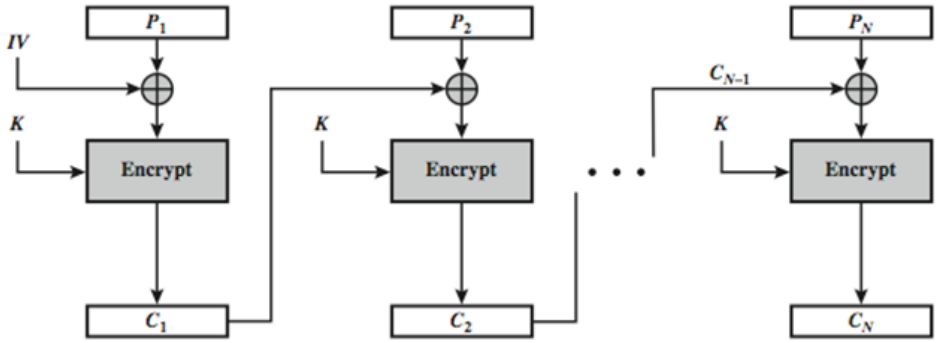
Шалгалт 3-5-р лекцийн хүрээнд ►

Question **1**

Answer saved

Marked out of 1.00

Дараах схем зургаар өгөгдсөн шифрлэх горимыг сонго



Select one:

- a. Cipher Block Chaining (CBC)
- b. Output FeedBack (OFB)
- c. Electronic Codebook Book (ECB)
- d. Counter (CTR)
- e. Cipher FeedBack (CFB)

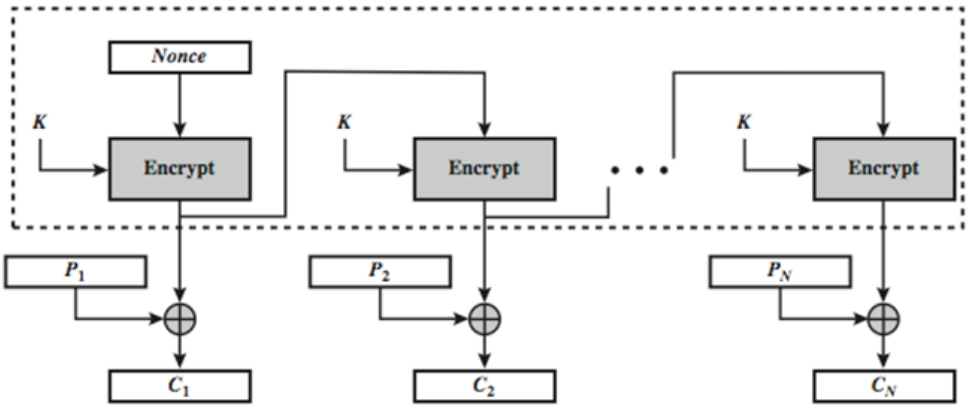
Clear my choice

Question **2**

Answer saved

Marked out of 1.00

Дараах схем зургаар өгөгдсөн шифрлэх горимыг сонго



Select one:

- a. Counter (CTR)
- b. Cipher Block Chaining (CBC)
- c. Cipher FeedBack (CFB)
- d. Electronic Codebook Book (ECB)
- e. Output FeedBack (OFB)

Clear my choice

Question **3**

Answer saved

Marked out of 1.00

Дараах томеогоор өгөгдсөн шифрлэх горимыг сонго

$O_i = E_K(i)$
$C_i = P_i$ XOR O_i

Select one:

- a. Electronic Codebook Book (ECB)
- b. Cipher FeedBack (CFB)
- c. Counter (CTR)
- d. Output FeedBack (OFB)
- e. Cipher Block Chaining (CBC)

Clear my choice

Question **4**

Answer saved

Marked out of 1.00

Дараах томеогоор өгөгдсөн шифрлэх горимыг сонго

$C_i = P_i \text{ XOR } E_K(C_{i-1})$
$C_{-1} = IV$

Select one:

- a. Output FeedBack (OFB)
- b. Cipher Block Chaining (CBC)
- c. Cipher FeedBack (CFB)
- d. Counter (CTR)
- e. Electronic Codebook Book (ECB)

Clear my choice

Question **5**

Answer saved

Marked out of 1.00

Дараах томеогоор өгөгдсөн шифрлэх горимыг сонго

$C_i = E_K(P_i)$

Select one:

- a. Output FeedBack (OFB)
- b. Counter (CTR)
- c. Cipher FeedBack (CFB)
- d. Cipher Block Chaining (CBC)
- e. Electronic Codebook Book (ECB)

Clear my choice

◄ Лаб 7 заавар

Jump to...

Даалгавар илгээх лаб 7 ►

Question **6**

Answer saved

Marked out of 1.00

Дараах томеогоор өгөгдсөн шифрлэх горимыг сонго

$C_i = E_K(P_i \text{ XOR } C_{i-1})$
$C_{-1} = IV$

Select one:

- a. Cipher Block Chaining (CBC)
- b. Cipher FeedBack (CFB)
- c. Output FeedBack (OFB)
- d. Counter (CTR)
- e. Electronic Codebook Book (ECB)

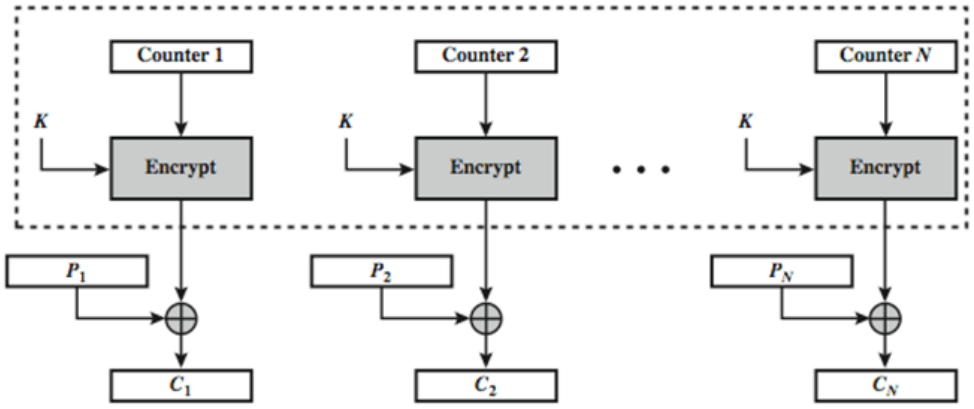
Clear my choice

Question **7**

Answer saved

Marked out of 1.00

Дараах схем зургаар өгөгдсөн шифрлэх горимыг сонго



Select one:

- a. Counter (CTR)
- b. Cipher FeedBack (CFB)
- c. Cipher Block Chaining (CBC)
- d. Output FeedBack (OFB)
- e. Electronic Codebook Book (ECB)

Clear my choice

Question **8**

Answer saved

Marked out of 1.00

Дараах томеогоор өгөгдсөн шифрлэх горимыг сонго

$O_i = E_K(O_{i-1})$
$C_i = P_i \text{ XOR } O_i$
$O_{-1} = IV$

Select one:

- a. Electronic Codebook Book (ECB)
- b. Output FeedBack (OFB)
- c. Cipher Block Chaining (CBC)
- d. Counter (CTR)
- e. Cipher FeedBack (CFB)

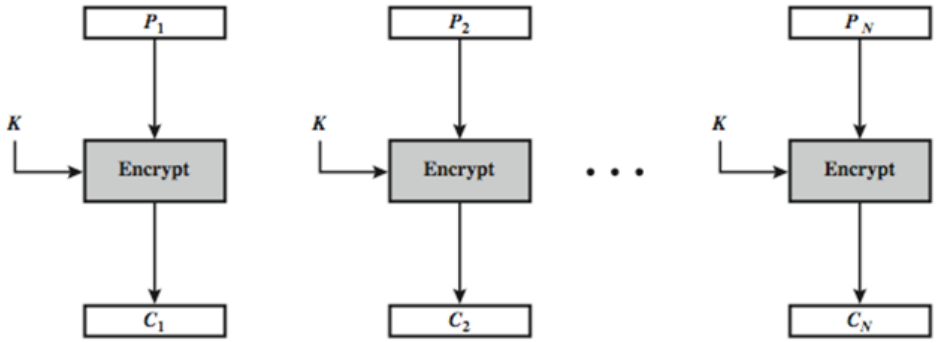
Clear my choice

Question **9**

Answer saved

Marked out of 1.00

Дараах схем зургаар өгөгдсөн шифрлэх горимыг сонго



Select one:

- a. Output FeedBack (OFB)
- b. Cipher FeedBack (CFB)
- c. Cipher Block Chaining (CBC)
- d. Counter (CTR)
- e. Electronic Codebook Book (ECB)

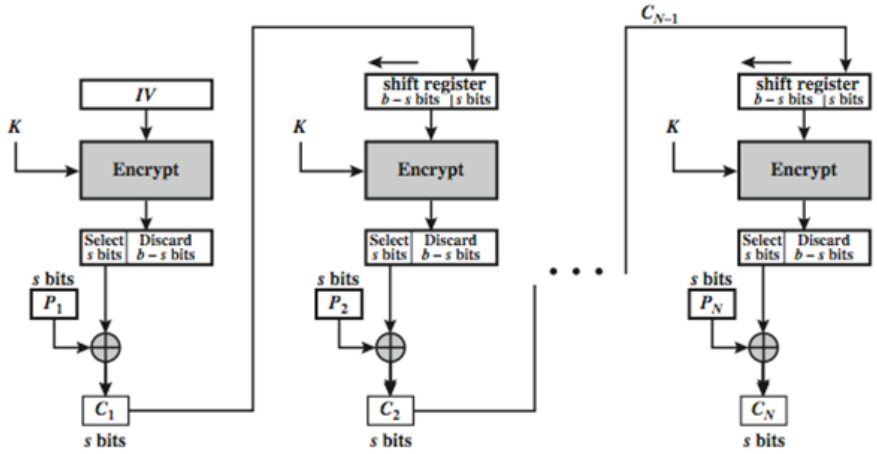
Clear my choice

Question **10**

Answer saved

Marked out of 1.00

Дараах схем зургаар өгөгдсөн шифрлэх горимыг сонго



Select one:

- a. Counter (CTR)
- b. Output FeedBack (OFB)
- c. Electronic Codebook Book (ECB)
- d. Cipher Block Chaining (CBC)
- e. Cipher FeedBack (CFB)

Clear my choice

◄ Лаб 7 заавар

Jump to...

Даалгавар илгээх лаб 7 ►

Crypto 8-13 soril

Дараах шугаман санамсаргүй тоо X_5-г ол

$a = 7,\ \ c = 0,\ \ m = 32,\ \ X_0 = 1$
$X_{n+1} = (7X_n + 0) \bmod 32$
X =7

Blum blum shub санамсаргүй тоо X_{14}-г ол

$n = 192649 = 383 * 503\ s= 101355$
$X_0 = s^2 \bmod n$
For i = 1 to q
$X_i = (X_{i-1})^2 \bmod n$
$B_i = X_i \bmod 2$
X =114386

Blum blum shub санамсаргүй тоо X_2-г ол

$n = 192649 = 383 * 503\ s= 101355$
$X_0 = s^2 \bmod n$
For i = 1 to q
$X_i = (X_{i-1})^2 \bmod n$
$B_i = X_i \bmod 2$
X=143135

Дараах шугаман санамсаргүй тоо X_2-г ол

$a = 7,\ \ c = 0,\ \ m = 32,\ \ X_0 = 1$
$X_{n+1} = (7X_n + 0) \bmod 32$
X =17

Аль нь анхны тоо вэ?
1367
Аль нь анхны тоо вэ?
181

Аль нь Ф(10)
4
Аль нь Ф(26)
12

RSA d-?, p = 3; q = 11, e = 7; M = 5
79

RSA C-?, p = 17; q = 31, e = 7; M = 3

79

RSA C-?, p = 11; q = 13, e = 11; M = 7

106

RSA d-?, p = 7; q = 11, e = 13; M = 8

37

RSA C-?, p = 7; q = 11, e = 17; M = 8

57

RSA d-?, p = 3; q = 11, e = 13; M = 5

23

RSA C-?, p = 3; q = 11, e = 7; M = 5

14

Diffie-Hellman Xa-?, a = 2; q = 11, Ya = 9
3

Diffie-Hellman Ya-?, Xa=5; q = 71, a = 7
51

Diffie-Hellman Xa-?, a = 3; q = 353, Ya = 40
97

Elgamal message=-?, p = 31; Xa=10, C(17,20)
H

Elgamal message=“HELLO”, 00-25 хүртэл үсгийг дугаарласан бол C2-?, p = 31; k = 7, a = 3, Ya=25, M="L"=11
27

Diffie-Hellman Yb-?, Xb=12; q = 71, a = 7
4

Elliptic Curve нэмэх үйлдэл 2P-?, E23(9,17),prime=23, P=(16,5)
(20, 20)

Elliptic Curve нэмэх үйлдэл 3P-?, E23(9,17),prime=23, P=(16,5)
(14, 14)

Elliptic Curve нэмэх үйлдэл 6P-?, E23(9,17),prime=23, P=(16,5)
(7, 33

Elliptic Curve нэмэх үйлдэл 7P-?, E23(9,17),prime=23, P=(16,5)
(8, 7)

Elgamal message=“HELLO”, 00-25 хүртэл үсгийг дугаарласан бол C2-?, p = 31; k = 7, a = 3, Ya=25, M="O"=14
09

Elgamal message=“HELLO”, 00-25 хүртэл үсгийг дугаарласан бол C2-?, p = 31; k = 7, a = 3, Ya=25, M="L"=11
27