№9 лекция тақырыбы: Гронсфельд шифры. Вижинер шифрлау жүйесі.

Лекцияның оқыту нәтижелері: Гронсфельд және Вижинер шифрларының жұмыс принципін, Кілттік сөз және кілттік тізбек ұғымдарын білу. Мәтінді Гронсфельд шифрымен шифрлау/дешифрлау және Вижинер кестесін пайдаланып мәтінді шифрлау және дешифрлауды орындайды.

Лекцияның мазмұны:

1. Гронсфельд шифрына қысқаша шолу
2. Вижинер шифрының тарихы
3. Гронсфельд шифрының Python бағдарламасында жүзеге асырылуы
4. Вижинер шифрының кестесі және жұмыс принципі
5. Ашық кілтті криптожүйелер туралы ұғым
6. RSA шифрлау жүйесі және шифрды ашу кезеңдері

1.1 Гронсфельд шифрына қысқаша шолу

Гронсфельд шифры - ПОЛИАЛФАВИТТІК қойылмалы шифрды XVII ғасырда Граф Гронсвельд (Германияның алғашқы шифрды ашу қызметінің жетекшісі) жасаған. Шифрды Цезарь (сенімділік) және Виженер / Бофор (жылдамдық) шифрын жетілдіру деп санауға болады. Бұл шифрлау әдісін 1854 жылы ағылшын физигі және плейфердің досы Чарльз Уитстон жасаған. Плейфердің еңбегі - ол мемлекеттік қызметте шифрды қолдануды сәтті насихаттаған жоқ.

Гронсфельд шифры – бұл вижинер шифрының қарапайым түрі, ол әліпбиді қайталамайтын цифрлық код арқылы шифрлауға негізделген. Бұл шифр әріптерді емес, тек цифрларды қолданады. Гронсфельд шифрының жұмыс принципі: Гронсфельд шифры – жасырын мәтінді (plain text) цифрлы кілт (key) арқылы шифрлау әдісі болып табылады. Кілттің әрбір цифры мәтіннің әрбір әрпін өзгерту үшін пайдаланылады.

Вижинер шифры – бұл көп мәртелі ауыстыру (polyalphabetic substitution) әдісі, ол қарапайым ауыстыру шифрларынан әлдеқайда күрделі әрі қауіпсіз. Вижинер шифры әліпбиі бойынша бірнеше алмастыру кестелерін пайдаланады. Вижинер шифрының жұмыс принципі: Вижинер шифры құпия кілтке негізделген және полиграфиялық ауыстыруды жүзеге асырады. Шифрлау процесінде әрбір әріптің шифрланған әріпке айналуы үшін сол әріптің орнына кілттің сәйкес әрпі таңдалады.

1.1 Гронсфельд шифрына қысқаша шолу

Гронсфельд шифры - ПОЛИАЛФАВИТТІК қойылмалы шифрды XVII ғасырда Граф Гронсвельд (Германияның алғашқы шифрды ашу қызметінің жетекшісі) жасаған. Шифрды Цезарь (сенімділік) және Виженер / Бофор (жылдамдық) шифрын жетілдіру деп санауға болады. Бұл шифрлау әдісін 1854 жылы ағылшын физигі және плейфердің досы Чарльз Уитстон жасаған. Плейфердің еңбегі-ол мемлекеттік қызметте шифрды қолдануды сәтті насихаттаған жоқ.

Гронсфельд шифры қалай жұмыс істейді?

Гронсфельд шифры-сандық кілт арқылы Цезарь шифрының модификациясы. Ол үшін бастапқы хабарламаның әріптерінің астына сандық кілт сандары жазылады. Егер кілт хабарламадан қысқа болса, онда оның жазбасы циклдік түрде қайталанады.

	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
0	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
1	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
2	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
3	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
4	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
5	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
6	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
7	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
8	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
9	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

1-сурет. Гронсфельд кестесі

Кілт ұзындығы (K) бастапқы мәтіннің ұзындығына тең болуы керек. Ол үшін кілт оның ұзындығы бастапқы мәтіннің ұзындығына сәйкес келгенше циклдік түрде жазылады. M ашық мәтінінің әрбір mi таңбасы Ki (сәйкес k кілт таңбасы) қадамдарын оңға жылжыту керек. Немесе Гронсфельд кестесін пайдалану (Tx y, мұндағы x-жол нөмірі, ал y-баған нөмірі және санақ нөлден басталады): c Шифр мәтінінің әрбір ci таңбасы y бағанының қиылысында орналасқан, оның бірінші (тақырып) таңбасы mi ашық мәтінінің сәйкес таңбасына тең және жолдың Ki-y (сәйкес кілт цифры) — (TKi y).

Шифрды ашу: Шифрланған c мәтінінің әрбір таңбасы (Ci) ki (сәйкес k кілт таңбасы) қадамдарын солға жылжыту керек. Немесе Гронсфельд кестесін пайдалану (Tx y, мұндағы x-жол нөмірі, ал y-баған нөмірі және санақ нөлден басталады): ki (i-ая k кілтінің цифры) жолында сәйкес Шифр мәтініне (TKi y = Ci) тең таңбаны табу керек, ал бағанның бірінші (тақырып) элементі i-ый ашық мәтін таңбасы болады.

Гронсфельд шифры-сандық кілт арқылы Цезарь шифрының модификациясы. Ол үшін бастапқы хабарламаның әріптерінің астына сандық кілт сандары жазылады. Егер кілт хабарламадан қысқа болса, онда оның жазбасы циклдік түрде қайталанады. Шифрмәтін Цезарь шифрындағыдай алынады, бірақ Алфавит бойынша үшінші әріп емес, Алфавит бойынша тиісті кілт санына сысқан әріпті таңдаңыз. Қалалық тапсырмаларға тапсырмалар жазу кезінде осы кодтауды жақсы қолдануға болады.

Граф Гронсфельд Германияда бірінші болып шифрды ашу бөлімін құрды. Ол сондай-ақ аттас шифрдың авторы. "Құпия" сөзін " 103 " кілтін пайдаланып шифрлағымыз келеді делік. Құпия сөзінің астына біздің кілтті циклдік түрде жазыңыз, содан кейін әр әріпті Алфавит бойынша төменде көрсетілгендей алға қарай жылжытыңыз, біз аламыз:

Т А Н А

1 0 3 1 0
A M O A

Тиісінше, шифрды шешу үшін алфавиттің ауысуы кері бағытта жүреді. Енді Гронсфельд шифрының тағы бір мысалы. Ағылшын таңбалары + әлі де бос орын бар, SOURCE CODE шифрлаңыз (аударма — "бастапқы код"). Шифрланған мәтіннің алғашқы 6 таңбасы әлі де болады TSWTDI, мысалдағыдай SOURCE сөзі және бос орын жоқ алфавит. Сонымен бірге біз 1422 кілтінің барлық сандарын бір рет қолдандық, сонымен қатар 1 және 4-ті екінші рет қолдануға тура келді. Әрі қарай, Гронсфельд шифрының алгоритмі бойынша біз екеуін қолданамыз. Кезекте бос орын бар, егер A 0 таңбасы болса, ол 26-шы. (26 + 2)mod 27 = 1, яғни бос орынның орнына B. енді C және кілттегі екінші екі. Егер A нөмірі 0 болса, онда C нөмірі 2 болады. (2 + 2) mod 27 = 4, яғни бұл E. әрі қарай, біз O шифрлаймыз, кілттің барлық сандары қолданылады, біз қайтадан ең үлкен (сол жақ) саннан бастаймыз, яғни 1-ге ауысу керек, O орнына P болады. және т. б…

1.2 Вижинер шифрының тарихы

Виженер шифры (фр. Chiffre de Vigenère) - кілт сөзді қолдана отырып, әріптік мәтінді полиалфавиттік шифрлау әдісі. Бұл әдіс көп алфавиттік ауыстырудың қарапайым түрі болып табылады. Виженердің шифры бірнеше рет ойлап табылды. Бұл әдісті алғаш рет Джованни Баттиста Беллазо la cifra del кітабында сипаттаған. Sig. Giovan Battista bellaso 1553 жылы, алайда XIX ғасырда француз дипломаты Блез Виженер есімін алды. Бұл әдісті түсіну және жүзеге асыру оңай, бірақ қарапайым криптоанализ әдістері қол жетімді емес. Шифрды түсіну және жүзеге асыру оңай болғанымен, үш ғасыр бойы ол оны бұзудың барлық әрекеттеріне қарсы тұрды, сондықтан оны "шешілмеген Шифр" деп атады (фр. le chiffre indéchiffrable). Көптеген адамдар шифрлау схемаларын жүзеге асыруға тырысты, олар негізінен Vigener шифрлары болды. 1466 жылы әйгілі сәулетші және философ Леон Альберти папа кеңсесіне шифрлар туралы трактат ұсынды. Трактат шифрлаудың әртүрлі тәсілдерін, соның ішінде кейбір қосалқы мәтіндегі ашық мәтінді бүркемелеуді қарастырады. Жұмыс өзінің шифрымен аяқталады, ол оны "патшаларға лайықты шифр"деп атады. Бұл шифрлау дискісі ретінде енгізілген көп алфавиттік шифр болды. Төменгі жол-бұл Шифр кілтке сәйкес бірнеше ауыстыруды қолданады. Кейінірек Альберти қайта шифрланған кодты ойлап тапты. Бұл өнертабыс өз уақытынан едәуір озып кетті, өйткені шифрдың бұл түрі Еуропа елдерінде 400 жылдан кейін ғана қолданыла бастады.

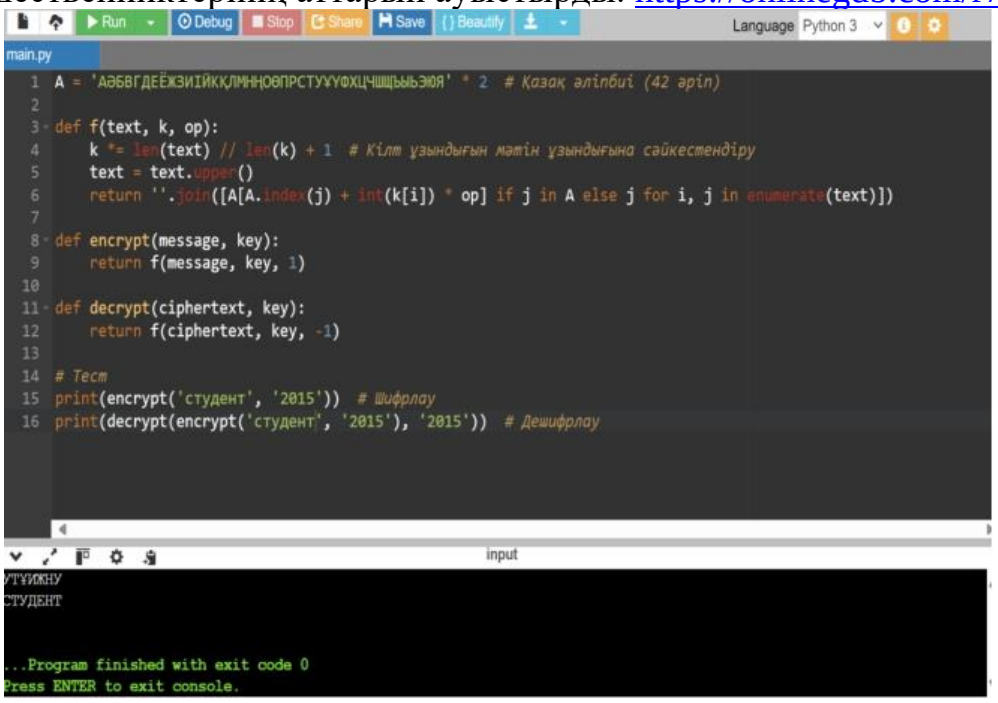
1518 жылы Германияда криптографияның алғашқы баспа кітабының пайда болуының арқасында криптографияның дамуына жаңа қадам жасалды. Вюрцбургтегі монастырьдің аббаты Иоганн Тритемиус бірқатар шифрлардың сипаттамасын беретін "Полиграфия" кітабын жазды. Олардың бірі "тритемия кестесін" (Қазіргі "Виженер кестесі") қолданады және көп алфавиттік ауыстыру идеясын дамытады. Шифрлау жүйесі келесідей: бастапқы мәтіннің бірінші әрпі бірінші жолда, екіншісі екінші жолда және т.б. шифрланады. Соңғы жолды қолданғаннан кейін келесі әріп бірінші жолда қайта шифрланады. Тритемия шифрында кілт жоқ, құпия-шифрлау әдісі. Тритемий

ұсынған шифрлау әдісін дамытудағы келесі қадамды итальяндық Джовани Белазо жасады. 1553 жылы оның "Синьор Белазо шифры"брошюрасы жарық көрді. Бұл шифрда кілт құпия сөз деп аталады-сөз тіркесі немесе сөз. Құпия сөз ашық мәтін әріптерінің үстінде мезгіл-мезгіл жазылып отырды. Ашық мәтіннің тиісті әрпінің үстінде тұрған пароль әрпі тритемия кестесіндегі жол нөмірін көрсетті, оны ауыстыру керек (шифрлау) бұл әріптер.

2.1 Гронсфельд шифрының python бағдарламасында коды

XVI ғасырдың ортасында Италияда Дж. Кардано" әр түрлі заттар туралы "қосымшасы бар"нәзіктіктер туралы". Онда криптографияның жаңа идеялары көрініс тапты: ең көп жіберілген ашық мәтіннің бір бөлігін Шифр кілті ретінде пайдалану ("өзін-өзі кілт" идеясы) және тарихқа "Кардано торы"ретінде енген шифрлаудың жаңа әдісі.

Францияның Римдегі елшісі Блез де Виженер тритемия, Белазо, Кардано, Порта, Альберти шығармаларымен танысып, криптографияға да қызығушылық танытты. 1585 жылы ол криптографияның негіздерін сипаттайтын "шифрлар туралы Трактат" жазды. Бұл жұмыста ол: "әлемдегі барлық нәрсе шифрды білдіреді. Барлық табиғат-бұл жай ғана Шифр және құпия хат". Бұл ойды кейінірек ықтималдық теориясының негізін қалаушылардың бірі Блез Паскаль, ал XX ғасырда Норберт Винер "кибернетиканың әкесі"ретінде қайталады. Шын мәнінде, Виженер Тритемия, Беллазо, Порт тәсілдерін ашық мәтіндерді шифрлауға біріктірді, оларға түпнұсқа ештеңе енгізбеді. Қазіргі уақытта тритемия кестесіндегі кілт сөздің мерзімді жалғасынан тұратын "Виженер шифры" оның предшественниктерінің аттарын ауыстырды. https://onlinegdb.com/r7aS7MTxJ



2-сурет.python бағдарламасында Гронсфельд шифрына мысал

2.2 Вижинер шифырының кестесі

Vigener квадраты сияқты көп алфавиттік жүйенің негізі ретінде қолдануға болатын көптеген басқа есте қаларлық квадраттар бар. Ең танымал бірі-Бофор алаңы. Оның жолдары-кері тәртіпте жазылған Vigener квадратының жолдары. Ол желдің жылдамдығын анықтау үшін масштабты жасаушы адмирал Сэр Фрэнсис Бофордың есімімен аталады. Егер Vigener квадратында бірінші жол мен баған сәйкесінше жолдар мен бағандарды көрсетсе, онда Бофор квадратында бірінші жол және соңғы баған осы мақсаттарға қызмет етеді. Іске қосу кілті бар Vigener шифрының нұсқасы[ағылш.] (ағылш. running key) бір кездері бұзылмайтын болды. Бұл нұсқа кілт ретінде бастапқы мәтіннің ұзындығына тең мәтін блогын пайдаланады. Кілт хабарламаның ұзындығына тең болғандықтан, Фридман мен Касиски ұсынған әдістер жұмыс істемейді (өйткені кілт қайталанбайды). 1920 жылы Фридман бұл нұсқаның кемшіліктерін бірінші болып ашты. Vigener шифрының running key мәселесі мынада: криптоаналитикте кілт туралы статистикалық ақпарат бар (мәтін блогы белгілі тілде жазылғанын ескере отырып) және бұл ақпарат шифрланған мәтінде көрсетіледі. Егер кілт шынымен кездейсоқ болса, оның ұзындығы хабарламаның ұзындығына тең және ол бір рет қолданылған болса, онда Vigener шифры теориялық тұрғыдан бұзылмайтын болады, іс жүзінде бұл опция Vernam Vigener шифры болады, ол үшін абсолютті криптовалюта дәлелденген.

Klartext

Schlüsselbuchstaben

	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Гронсфельд шифры мен Вижинер шифры екеуі де ауыстыру шифрларының өзгерген түрлері болып табылады, бірақ Вижинер шифры әлдеқайда қауіпсіз әрі күрделі. Гронсфельд шифры тек цифрлармен шифрлау жасағанымен, Вижинер шифры толыққанды әріптермен жұмыс істейді, бұл оны көптеген мәтіндер үшін тиімді етеді. Гронсфельд және Вижинер шифрлары – классикалық шифрлау әдістері, олардың негізі көп мәртелі ауыстыру (polyalphabetic substitution) және қарапайым ауыстыруға негізделген. Гронсфельд шифры өз қарапайымдылығымен ерекшеленеді, себебі ол тек цифрларды пайдаланып, әріптердің орнына олардың сандық мәндерін қолданады. Бұл шифрдың тиімділігі оның қарапайымдылығында болса да, қазіргі таңда ол көптеген қауіпсіздік қатерлеріне төтеп бере алмайды. Сондықтан Гронсфельд шифры көбіне оқытушы мақсатында немесе тарихи әдіс ретінде қолданылады. Вижинер шифры өзінің күрделілігі мен қауіпсіздігі арқасында алдыңғы шифрлардан әлдеқайда жоғары. Ол алфавит бойынша әріптердің бірнеше ауыстыруларын қолдана отырып, мәтінді шифрлайды, бұл оның қауіпсіздігін арттырады. Алайда, кілттің ұзындығы мен оның кездейсоқтығы өте маңызды рөл атқарады. Вижинер шифры қазіргі таңда криптографияда кеңінен қолданылмағанымен, оның тарихта орын алған ықпалы үлкен. Екі шифрдың да негізгі кемшіліктері – олар тек мәтіннің құрылымын өзгертіп, мәтінді қорғауға бағытталған, бірақ қазіргі криптографиялық жүйелерге қарағанда әлдеқайда осал болып табылады. Бұл шифрларды пайдалану үшін күшті кілттер мен қосымша қауіпсіздік шаралары қажет. Қорыта айтқанда, Гронсфельд және Вижинер шифрлары қазіргі криптографиялық әдістердің негізін қалаған, бірақ оларды қазіргі заманғы қауіпсіздік талаптарына сай деп айту қиын.

Негізгі құралы:
Вижинер кестесі (Тритемий кестесі)

Оқытудың техникалық құралдары:
Интерактивті тақта, компьютер, презентация, маркер.

Лекция оқудың тәртібі, оқыту әдістері мен түрлері:
Түсіндіру, мысалды талдау, сұрақ-жауап, ашық мәтінді шифрлау, топтық жұмыс.

Әртүрлі күрделілік деңгейдегі тапсырмалар (сұрақтар) және бағалау үлестірілуі:
1. Күрделі деңгей (3 ұпай):
– Берілген сөйлемді Вижинер шифрымен шифрлаңыз (кілтті студент өзі таңдайды).
2. Орта деңгей (2 ұпай):
– «ҚАЗАҚСТАН» сөзін «31425» кілтімен Гронсфельд шифры арқылы шифрлаңыз.

3. Жеңіл деңгей (1 ұпай):
– Көпалфавиттік шифрлау дегеніміз не?

БӨЖ және ОБӨЖ тапсырмалары,олардың түрлері мен орындалуына қойылатын ұпайлардың үлестері:

БӨЖ: Гронсфельд және Вижинер кестесі арқылы шифрлау мысалдарын орындау, берілген мәтінді шифрлап және дешифрлап орындауы қажет. Бұл жұмыс жалпы бағалаудың 60-баллды құрайды.

БӨЖ бағалау критерийлері:

- Теориялық материалды түсіну және қолдану -15 балл
- Бағдарламаны дұрыс жазу немесе есепті шешу -30 балл
- Нәтижелердің дәлдігі мен түсіндіру сапасы -15 балл

Барлығы: 60 балл

ОБӨЖ: Гронсфельд және Вижинер кестесі арқылы шифрлау алгоритмін қолданып мәтінді шифрлау және екі әдістің айырмашылығын талдау бойынша қысқаша есеп дайындау. Бұл жұмыс жалпы бағалаудың 40-баллды құрайды.

ОБӨЖ бағалау критерийлері:

- Тапсырманың толық және уақытылы орындалуы -15 балл
- Теориялық және практикалық түсіндіру сапасы -15 балл
- Топтық жұмысқа белсенді қатысу, сұрақтарға жауап беру-10 балл

Барлығы: 40 балл

Жалпы бағалау үлесі:

- БӨЖ — 60% (60 балл)
- ОБӨЖ — 40% (40 балл)

Негізгі әдебиеттер:

1. Г. Камалова, А. Х. Касымова, Л. Б. Диярова. «Ақпараттық қауіпсіздікті басқару». Оқу құралы. – Алматы: Альманахъ, 2020. – 128 с.

2. Дүйсебекова К. С. Ақпараттық қауіпсіздік және ақпараттарды қорғау. Оқу құралы. – Алматы: Қазақ университеті, 2013. – 156 с.

Қосымша әдебиеттер:

1. Ахметова С. Бағдарламалау технологиясы. Лекция жинағы. – Шымкент: ОҚМУ, 2007. – 51 б. https://rmebrk.kz/book/50006

2. Сатмаганбетова Ж.З. Бағдарламалау тілдері және технологиясы. Оқу-әдістемелік құралы. – Қостанай: ҚМУ, 2014. – 64 б. http://rmebrk.kz