

Студенттердің өзіндік жұмыстары. (СӨЖ)

№ к/ к	Тапсырма	Өткізу формасы	Әдістемелік ұсыныс	Ұсынылаты н әдебиеттер
1	Ақпаратты қорғаудың заңдық көзқарасы.	Эссе түрінде	Жалпы түсініктер. Қазақстан Республикасының ақпаратты қорғау туралы заңы	[7]-2- 15 б.
2	Компьютерлік жүйелердегі ақпарат қауіпсіздігі.	Эссе түрінде	АСӨЖ-ның негізгі қаупі. АСӨЖ қауіпсіздігін қамтамасыз ету.	[2]-23- 31 б.
3	Ақпаратты қорғаудың криптографиялық әдісі.	Баяндама	Терминология . Криптографиялық жүйелерге талаптарды талдау. Криптографиялық жүйелерді классификациялау.	[2]- 37-73 б. [7]-16- 33 б.
4	Жалғанкездейсоқ сандар тізбектерін генерациялайтын сызықты рекурентті қатынастар әдісі.	Рецензиялау	Вариант бойынша жалғанкездейсоқ сандар тізбектерін генерациялайтын сызықты рекурентті қатынастар әдісін қолдану.	[2]–73- 81 б.
5	DES алгоритмі.	Слайд қорғайды	Берілген әдебиет бойынша материалдар жинап, варианттар бойынша мәтіндерді шифрлау	[2]-83- 92 б. [3] – 209- 219 б.

			және шифрды ашу.	
6	Блоктық шифрларды қолдану режимі.	Пікірталас	Берілген әдебиет бойынша материалдар жинап, варианттар бойынша мәтіндерді шифрлау және шифрды ашу.	[2] - 46- 47 б. [5] – 125-128 б.
7	AES – RIJNDAEL криптографиялық қорғаудың стандарты.	Эссе түрінде	Шифра құрлымы. Математикалық негіздер.	[4] - 193- 206 б.
8	Ағымдық шифрлар.	Эссе түрінде	Ағымдық RC4 шифрі. A5 шифрлар жүйесі.	[3]-247-250 б. [4]-186-193 б.
9	Модулярлық арифметика	Баяндама	Вариант бойынша кез келген а санның дәрежесін n модулі бойынша есептеу.	[2] – 301-305 б.
10	Кері мөлшерлерді есептеу.	Рецензиялау	Вариант бойынша кері шамаларды үш тәсілмен есептеу.	[2] -305-310 б.
11	RSA криптожүйесінде шифрлау және шифрды алу процедуралары.	Слайд қорғайды	Вариант бойынша RSA алгоритмін қолданып мәтіндерді шифрлау және шифрды ашу.	[2] –131-133 б.
12	Эль-Гамаль шифрлауының сұлбасы.	Пікірталас	Вариант бойынша Эль Гамаль алгоритмін қолданып мәтіндерді шифрлау және шифрды ашу.	[2] - 136-137 б.

13	Бір бағыттағы хэш-функциялар.	Эссе түрінде	Қауіпсіз хэштеу SHA алгоритмі. Бір бағыттағы хэш-функцияларын қолдана отырап симметриялық блокті алгоритм құру.	[2] - 154-162 с.
14	Электронды сандық қолтаңбаның алгоритмі.	Эссе түрінде	Берілген әдебиет бойынша материалдар жинап, варианттар бойынша мәтіндерді шифрлау және шифрды ашу.	[2] - 162-171 б.
15	Эль-Гамаль сандық қолтаңбасының алгоритмі.	Баяндама	Берілген әдебиет бойынша материалдар жинап, варианттар бойынша Эль-Гамаль алгоритмімен мәтіндерді шифрлау және шифрды ашу.	[2] - 165- 166 б.