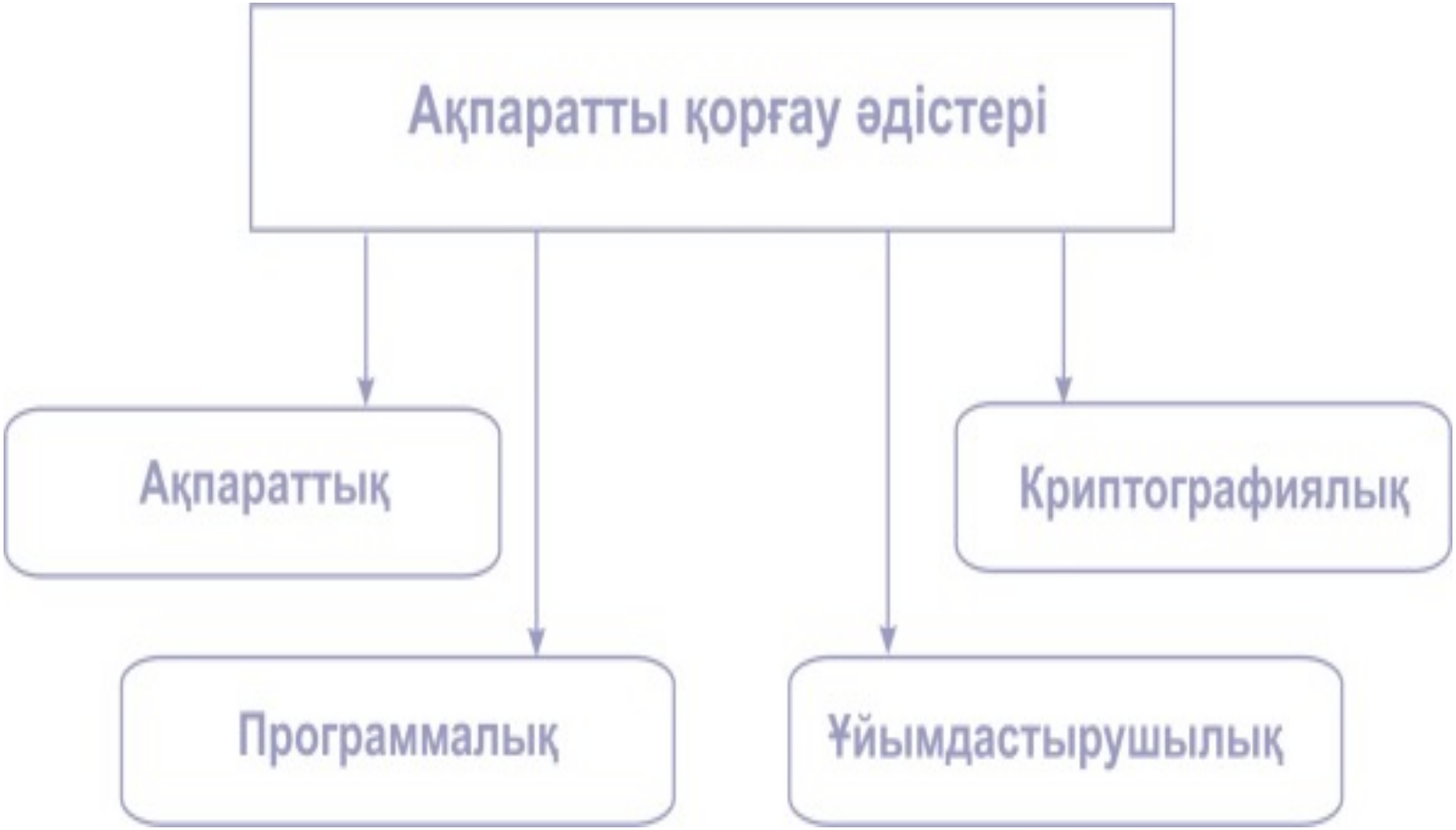
Ақпаратты қорғаудың криптографиялық әдістері


Ақпаратты қорғау әдістері
Ақпараттық
Криптографиялық
Программалық
Ұйымдастырушылық

Криптография деген не?

Криптография *- грек тілінен аударғанда κρυπτός — құпия және γράφω — жазу дегенді білдіреді.*

Яғни ***криптография*** *дегеніміз ақпараттың құпиялылығын (бөгде адамдардың ақпаратты оқып қоюына мүмкіндік бермейтін) қамтамасыз ететін ғылым деуге болады.*

Ақпаратты қорғаудың криптографиялық әдісі

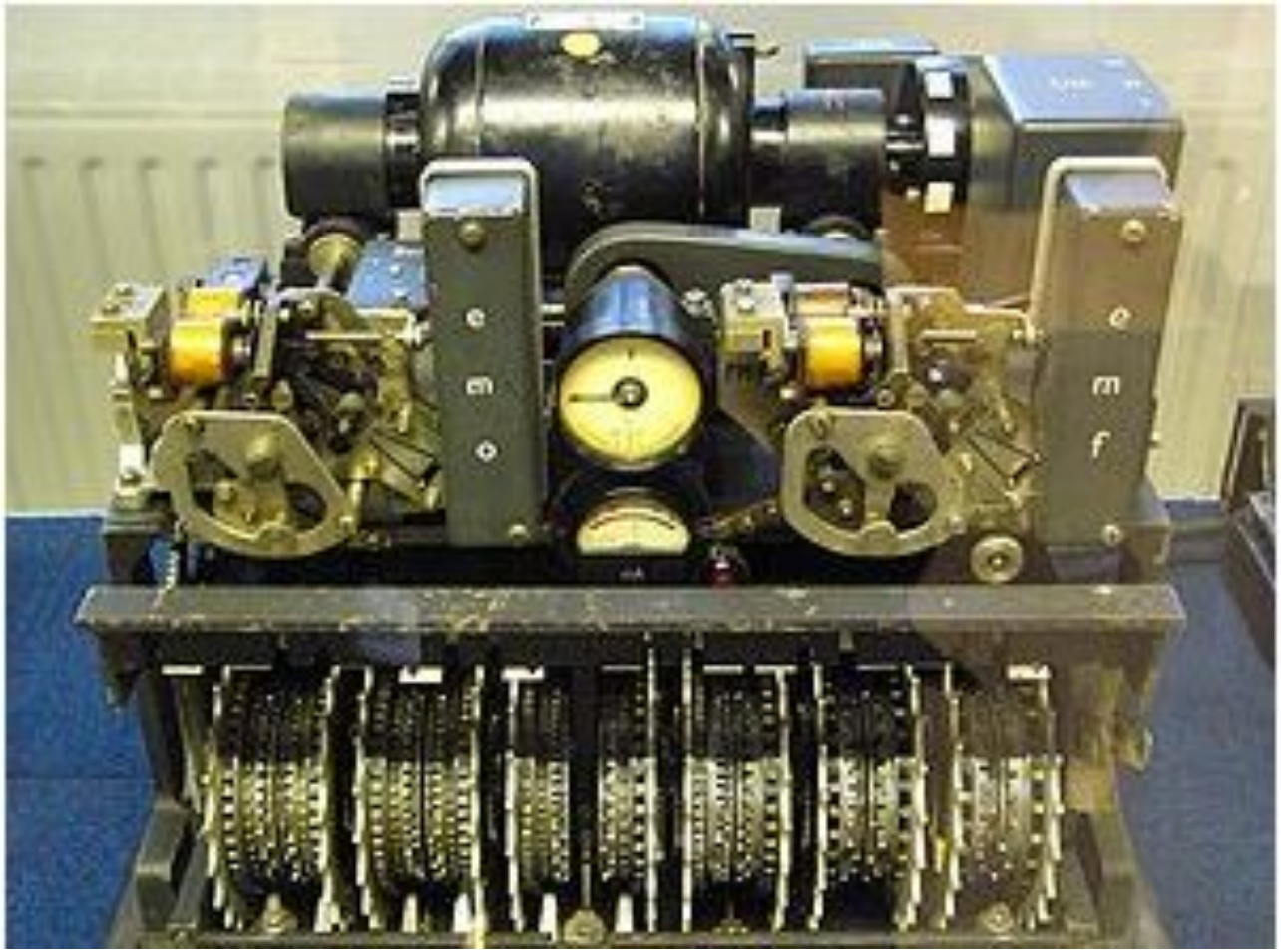
Ақпаратты қорғаудың криптографиялық әдісі – бұл ақпаратты шифрлаудың, кодтаудың немесе басқаша түрлендірудің арнайы әдісі, мұның нәтижесінде ақпарат мазмұнына криптограмма кілтінсіз және кері түрлендірмей шығу мүмкін болмайды.

Криптографиялық қорғау – ең сенімді қорғау әдісі, өйткені ақпаратқа шығу емес, оның тікелей өзі қорғалады.

Тарихи деректерден

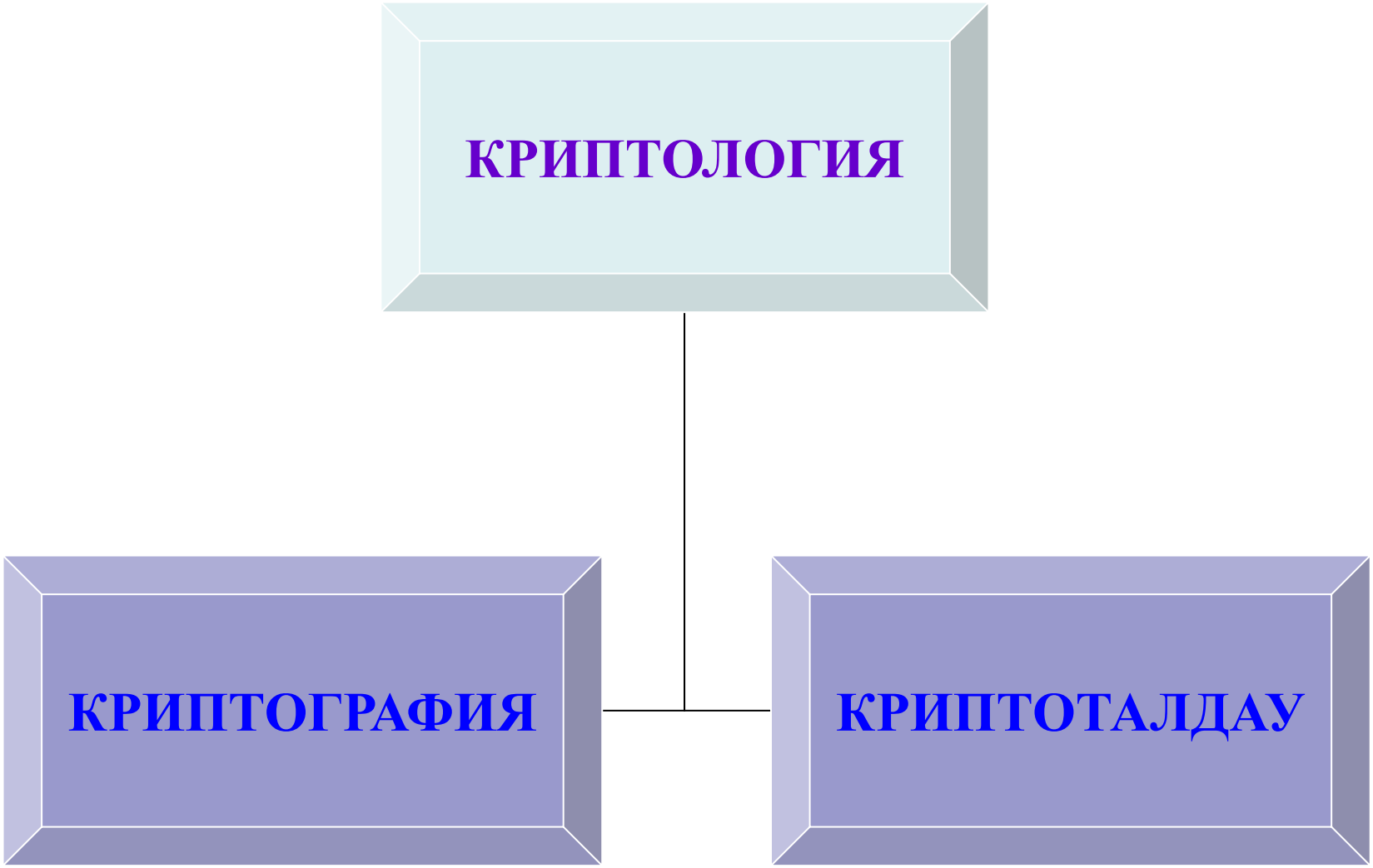
- Ақпаратты өзгерту арқылы қорғау – адамзатты ерте заманнан ойландырып келе жатқан проблеманың бірі. Криптография тарихы адамзат тілі тарихымен шамалас. Сонымен бірге алғашқы жазбаның өзі де криптографиялық жүйе болып саналады, себебі оны ежелгі қоғамда тек таңдаулы адамдар ғана игере білді. Оған Ежелгі Египеттің, Ежелгі Үндінің қасиетті кітаптары мысал бола алады.
- Жазба өнерінің кең таралуы криптографияның өзіндік ғылым ретінде қалыптасуына себеп болды. Алғашқы криптожүйелер біздің эрамызға дейінгі кезеңде де кездеседі. Бірінші және екінші дүниежүзілік соғыс жылдарында криптожүйелер дамуы қарқынды өріс алды. Автоматтандырылған жүйелердегі ақпараттарды қорғау үшін қолданылады. Қазіргі кезде ақпараттық жүйелердегі криптографиялық әдістерді қолдану неліктен көкейкесті мәселе болып отыр.
- Себебі, бір жағынан бөгде адамдардың оқуына мүмкіндік бермейтін үлкен мемлекеттік, әскери, коммерциялық және жеке түрдегі көлемді ақпараттар берілетін компьютерлік желілерді, соның ішінде глобалды желі Интернетті пайдалану кеңейді.

Немістің Lorenz атты криптомашинасы Екінші дүниежүзілік соғыс уақытында ең құпия деген хабарламаларды шифрлау үшін қолданылды.



«Энигма» роторлы шифрлау машинасы

Бұл роторлы шифрлау машинасының түрлі модификацияларын герман әскерлері 1920 жылдардың соңынан бастап Екінші дүниежүзілік соғыстың соңына дейін қолданып келді.


КРИПТОЛОГИЯ
КРИПТОГРАФИЯ
КРИПТОТАЛДАУ

Криптология *– екі бағытқа бөлінеді, криптография және криптоталдау. Бұл бағыттардың мақсаты бір-біріне қарама-қайшы.*

Криптография *ақпаратты түрлендірудің материалдық әдістерін зерттеумен және іздеумен айналысады.*

Криптоталдау *аймағына – кілтті білмей-ақ ақпаратты ашу (расшифрования) мүмкіндіктерін зерттеу жатады.*

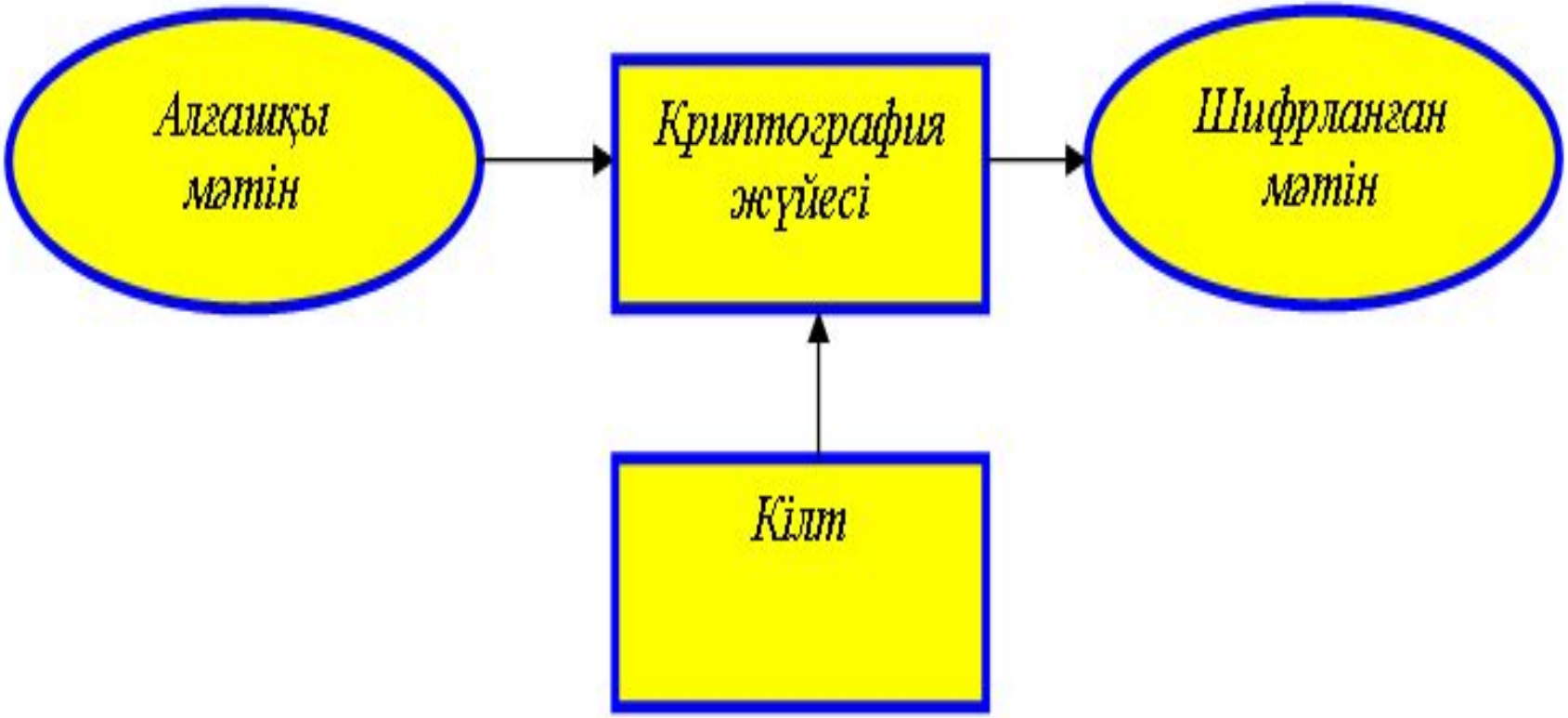
КРИПТОГРАФИЯНЫҢ ТҮРЛЕРІ

- Симметриялық криптожүйелер
- Ашық кілтті криптожүйелер
- Электрондық жазба жүйесі
- Кілтті басқару

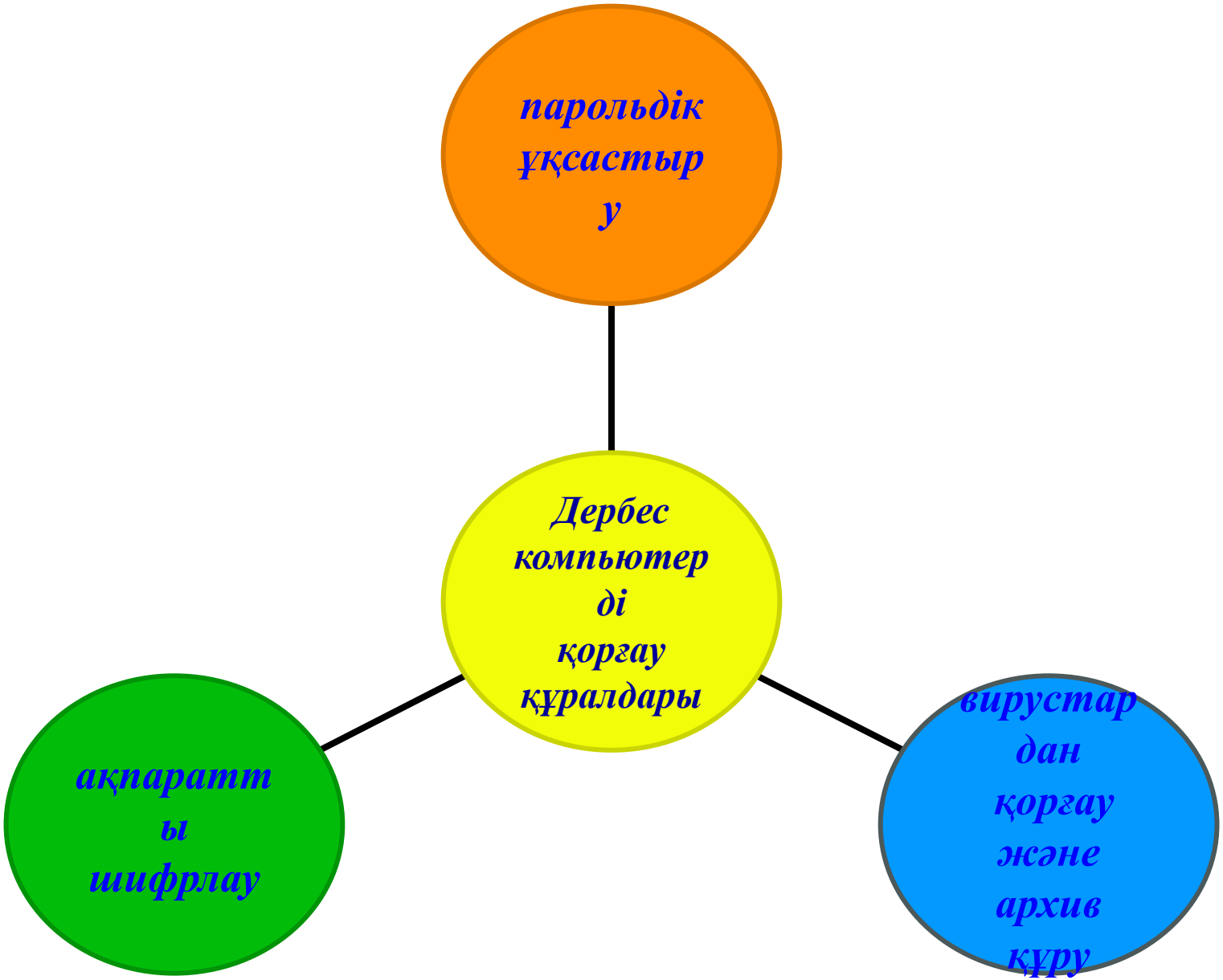
Не себепті криптографияны қолданады

Дербес компьютерді жергілікті желіге қосып пайдалану мүмкіндігі немесе телефон арқылы ақпарат алмасу үшін «модем» қолдану дербес компьютер ақпаратын қорғаудың программалық қамтамасыз етуіне қатаң талап қояды. Әр түрлі мекемелердегі дербес компьютер тұтынушылары ақпарат алмасу үшін электрондық поштаны кеңінен қолданбаса, бөгде адамдарға белгілі болып қалуы мүмкін. Дербес компьютердің программалық өнімі мен жіберілетін ақпаратқа рұқсатсыз шығудан ең сенімді қорғау - әр түрлі шифрлау әдісін, яғни ақпарат қорғаудың криптографиялық әдістерін қолдану болып табылады.

Файлды шифрлау процесі



Симметриялық криптожүйелердің түрлері


парольдік ұқсастыру
Дербес компьютерді қорғау құралдары
ақпаратты шифрлау
вирустардан қорғау және архив құру

2.4. Құжаттарды, жұмыс кітаптарын және көрсетілімдерді құпия сөзбен қорғау

2007 Microsoft Office шығарылымында басқа адамдардың Microsoft Office Word 2007 құжаттарын, Microsoft Office Excel 2007 жұмыс кітаптары мен Microsoft Office PowerPoint 2007 көрмелерін ашуына немесе өзгертуіне жол бермеу үшін құпия сөздерді орнатуға болады.

Құпия сөз үшін бас және кіші әріптерден, сандардан және таңбалардан тұратын қиын кілт сөздерді пайдалану қажет. Жеңіл кілт сөзде ондай қасиеттер жоқ. Қиын кілт сөз үлгісі: Y6dh!et5. Жеңіл кілтсөз: Үй27. кілт сөздердің ұзындығы 8 немесе одан да көп таңбадан тұруы тиіс. 14 немесе одан да көп таңбадан тұратын кілт сөйлемдер ең жақсы шешім болып табылады. Кілт сөзіңізді жатқа білген өте маңызды. Кілт сөзіңізді ұмытып қалсаңыз, Microsoft корпорациясы оны қалпына келтіре алмайды. Кілт сөзіңізді жазып қойып, өзі қорғауға арналған ақпараттан аулақ, қауіпсіз жерде сақтаңыз.

Құжатты шифрлау және оны ашуға құпия сөз орнату

Файлды шифрлау және оны ашуға құпия сөз орнату үшін мына әрекетті орындаңыз:

Microsoft Office түймешігін басып, меңзерді *Дайындау* пәрменіне апарып, одан кейін *Құжатты шифрлау* параметрін таңдаңыз.

Құжатты шифрлау тілқатысу терезесіндегі *Құпия сөз* жолағына құпия сөзді теріп, *ОК* түймешігін басыңыз.

255-ке дейін таңба тере аласыз. Әдепкіде, бұл мүмкіндік AES 128-биттік қосымша шифрлауды пайдаланады. Шифрлау — файлды қауіпсіз етуге көмектесетін стандартты әдіс.

Жазба кілтін және оқу кілтін пайдалана отырып, кесте бойынша күрделендірілген орын ауыстыру әдісі

Матрицаның жолға жазылу тәртібін жазбаның кілті деп атайық, ал шифрограмманы бағана бойынша оқу тәртібін – оқу кілті.

n х *n* өлшемді матрицаның көмегімен алынған криптограмманы кері шифрлау үшін бұл криптограмманы әр топқа *n* символ бойынша символдар топтарына бөлу керек. Шеткі сол жақтағы топты нөмірі оқудың бірінші сандық кілтпен сәйкес келетін бағанаға жоғарыдан төмен жазу керек. Символдардың екінші тобын нөмірі оқудың екінші сандық кілтімен сәйкес келетін бағанаға жазу керек, және т.с.с. Ашық мәтінді жазба кілтінің сандарымен сәйкес жол бойынша мартицадан оқу керек.

	1	2	3	4	5	6
1	Т	Ә	У	Е	Л	С
2	І	З	Д	І	К	-
3	Қ	А	З	А	Қ	-
4	Х	А	Л	Қ	Ы	Н
5	Ы	Ң	-	А	Қ	-
6	А	Р	М	А	Н	Ы

Жазба кілтін және оқу кілтін пайдалана отырып, кесте бойынша күрделендірілген орын ауыстыру әдісі

Орын ауыстыру әдісімен алынған криптограмманың кері шифрлау мысалын қарастырайық. Шифрлау кезінде 6х6 өлшемді матрица, 364215 жазба кілті және 364215 оқу кілті қолданылғаны белгілі. Яғни жазба кілті мен оқу кілті бірдей болса, онда шифрлауды мына тәртіппен жүргіземіз. Шифрограмманың мәтіні мынадай:

УДЗЛ_МС_ _Н_ЫЕІАҚААӘЗААҢРТІҚХЫАЛКҚЫҚН

Шифрограмманы 6 символ бойынша топтарға бөлейік:

УДЗЛ_М С_ _Н_Ы ЕІАҚАА ӘЗААҢР ТІҚХЫА ЛКҚЫҚН

3 6 4 2 1 5

Символдардың бірінші тобын 4 матрицаның бағанасына жазайық, себебі оқу кілтінің бірінші саны – 4. 6 символдан тұратын екінші топты 2 бағанасына жазайық, символдардың үшінші тобын – 5 бағанаға және т.с.с.

Кілттегі цифрлар бағандардың ретін көрсетеді. Яғни бірінші 3 бағандағы 6 символ, одан соң 6 бағандағы 6 символ, одан кейін 4 баған, 2 баған, 1 баған, және ең соңында 5 бағандағы символдар бір-бірінің соңына тіркестіріліп жазылады.

	1	2	3	4	5	6
1	Т	Ә	У	Е	Л	С
2	І	З	Д	І	К	-
3	Қ	А	З	А	Қ	-
4	Х	А	Л	Қ	Ы	Н
5	Ы	Ң	-	А	Қ	-
6	А	Р	М	А	Н	Ы

Оқу кілтін пайдаланып кері шифрлау әдісі

	1	2	3	4	5	6
1			У			С
2			Д			-
3			З			-
4			Л			Н
5			-			-
6			М			Ы

	1	2	3	4	5	6
1			У	Е		С
2			Д	І		-
3			З	А		-
4			Л	Қ		Н
5			-	А		-
6			М	А		Ы

	1	2	3	4	5	6
1		Ә	У	Е		С
2		З	Д	І		-
3		А	З	А		-
4		А	Л	Қ		Н
5		Ң	-	А		-
6		Р	М	А		Ы

	1	2	3	4	5	6
1	Т	Ә	У	Е		С
2	І	З	Д	І		-
3	Қ	А	З	А		-
4	Х	А	Л	Қ		Н
5	Ы	Ң	-	А		-
6	А	Р	М	А		Ы

Орын ауыстыруды кесте бойынша күрделендіргенде шифрдың беріктігін жоғарылату үшін орын ауыстыру кестесіне кестенің пайдаланылмайтын ұяшықтары енгізіледі. Пайдаланылмайтын элементтердің жалпы саны мен орналасуы шифрлаудың қосымша кілті болып табылады.

Түсіндіру үшін 8х8 өлшемді квадраттық кестені (матрицаны) алайық, мәтінді жүйелі түрде жол бойынша жоғарыдан төмен жазамыз да жүйелі түрде бағана бойынша солдан оңға қарай оқимыз.

Мына хабарламаны шифрлау керек деп есептейік:

Біздің басты құндылығымыз – Тәуелсіздік, Бейбітшілік пен Тұрақтылық

Осы хабарламаның матрицасын жазайық:

Матрицада «_» символымен бос орын белгіленеді.

	1	2	3	4	5	6	7	8
1	Б	І	З	Д	І	Ң	-	Б
2	А	С	Т	Ы	-	Қ	Ұ	Н
3	Д	Ы	Л	Ы	Ғ	Ы	М	Ы
4	З	-	Т	Ө	У	Е	Л	С
5	І	З	Д	І	К	-	Б	Е
6	И	Б	І	Т	Ш	І	Л	І
7	К	-	П	Е	Н	-	Т	Ұ
8	Р	А	Қ	Т	Ы	Л	Ы	Қ

ҚОРЫТЫНДЫ

Сондықтан қазіргі информациялық қоғамдағы өмірге балаларды дайындау үшін олардың тек логикалық ойлау қабілетін, анализ және синтез жасау мүмкіндіктерін ғана дамытып қоймай, қазіргі кездегі оқыту процесінің ең маңызды бөлігі – информациялық мәдениет элементтерін бойларына сіңдіріп, ұғындыру керек. Ағыл-тегіл информация заманында өмір сүретін адам бастауыш мектептің өзінде-ақ өзін-өзі шектей білетін негізгі нормалар мен ережелерді игеруі тиіс. Оның бойында жас кезінен информациялық объектілер мен процестерге оның ішінде компьютерлік ойындар мен вирустарға да қатысты пайдалы әдеттер мен әлеуметке жат әрекеттерге деген дұрыс көзқарасы қалыптасуы керек. Сондай-ақ кез келген бала компьютерлік ақпаратты қорғау тәсілдерінен хабардар болып, қарапайым тұтынушы деңгейінде криптографиялық жүйелерді қолдануды білуі шарт деп есептеймін.