Дәріс 3

Деректерді қорғаудың криптографиялық құралдары

Шифрлеу

- **Шифрлеу** – қауіпсіздіктің криптографиялық сервисін пайдалану.
- **Шифрлеу процедурасы**– хабарламаның ашық мәтінін жабыққа түрлендіру.
- Шифрлеудің қазіргі құралдары шифрлеудің белгілі алгоритмдерін қолданады. Түрленген хабарламаның жасырындылығын (конфиденциалдылығын) қамтамасыз ету үшін түрлендірудің арнайы параметрі – кілттер пайдаланылады.

Шифрлеу

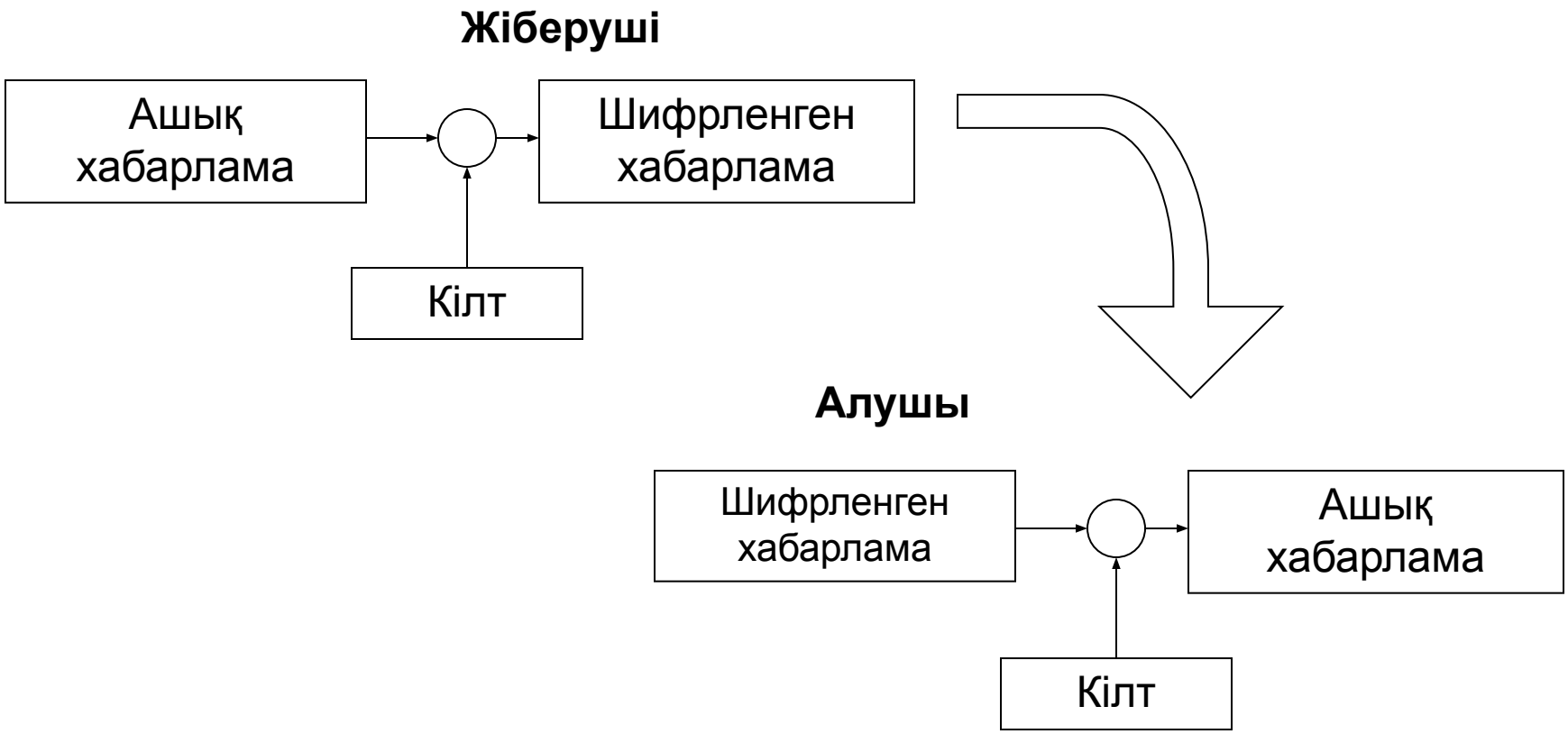
- Криптографиялық түрлендірулер қауіпсіздіктің келесі сервистерін қалыптастыру үшін қолданылады:
  - Шифрлеу (деректер конфиденциалдылығын қамтамасыз ету);
  - Бүтіндікті бақылау;
  - Аутентификация.

Ақпаратты криптографиялық қорғау жүйелері

- Ақпаратты криптографиялық қорғау құралдарының міндеті – ақпараттық объектілерді қандайда бір математикалық алгоритм көмегімен түрлендіру.
- Ширфлеу процесі объект – ашық мәтін және объект – кілт енуші параметр ретінде пайдаланылады, ал түрлендіру нәтижесі – объект – шифрленген мәтін. Дешифрлеу кезінде кері процесс орындалады.
- АЖ-де криптографиялық әдіске қандайда бір арнайы алгоритм сәйкес келеді. Берілген алгоритмді орындау кезінде әмбебап сандық мәні - **кілт** қолданылады.
- Кілт мәні кері түрлендіруді орындауға және ашық хабарлама алуға мүмкіндік береді.
- Криптографиялық жүйенің төзімділігі қолданылатын алгоритмдермен және кілттің құпиялық дәрежесімен анықталады.

Деректердің қорғаудың криптографиялық құралдары

- Ақпаратты қорғауды қамтамасыз ету үшін ақпаратты қорғаудың криптографиялық құралдары белсенді қолданылуда.
- Криптографиялық әдістер мәні келесіден тұрады:



АҚ (ИБ) қауіптерін алдын-алуға арналған криптографиялық қорғау құралдарын пайдалану

- **Деректердің жасырындылығын қамтамасыз ету**. Криптографиядық алгоритмдерді пайдалану ақпараттың ұрлануын алдын алуға мүмкіндік береді. «Қаскүнемде» кілттің болмауы шифрленген ақпаратты ашуға мүмкіндік бермейді;
- **Деректердің бүтіндігін қамтамасыз ету**. Симметриялық емес шифрлеу алгоритмдерін пайдалану ақпарат бүтіндігін бақылау әдістерін құруды мүмкін етеді.
- **Электронды цифрлік қолтаңба.** Ақпараттан бас тарту мәселелерін шешуге мүмкіндік береді.
- **Аутентификацияны қамтамасыз ету**. Криптографиялық әдістер аутентификацияның әр түрлі схемаларында қолданылады.

Криптожүйелерге қойылатын талаптар:

- 1. Шифрленген хабар тек кілт болғанда ғана оқылуы тиіс.
- 2. Шифрленген хабар фрагменті бойынша шифрлеудің қолданылған кілтін анықтау үшін қажетті операциялар саны және оған сәйкес ашық мәтін мүмкін болатын кілттердің жалпы санынан аз болмауы керек.
- 3. Барлық мүмкін болатын кілттерді артық таңдау жолымен ақпараттарды шифрлеуді ашу үшін қажетті операциялар саны қатал төмен бағамен болуы тиіс және қазіргі компьютерлердің мүмкіндіктерінің (тораптық есептеу мүмкіндіктерін ескере отырып) шегінен шығуы керек.
- 4. Шифрлеу алгоритмін білу қорғау сенімділігіне әсер етпеуі тиіс.
- 5. Кілттің аздап өзгеруі бір кілтті ғана қолданғанның өзінде шифрленген хабар түрінің елеулі өзгеруіне әкелуі тиіс.
- 6. Шифрлеу алгоритмінің құрылымдық элементтері өзгеріссіз болуы керек.

Криптожүйелерге қойылатын талаптар:

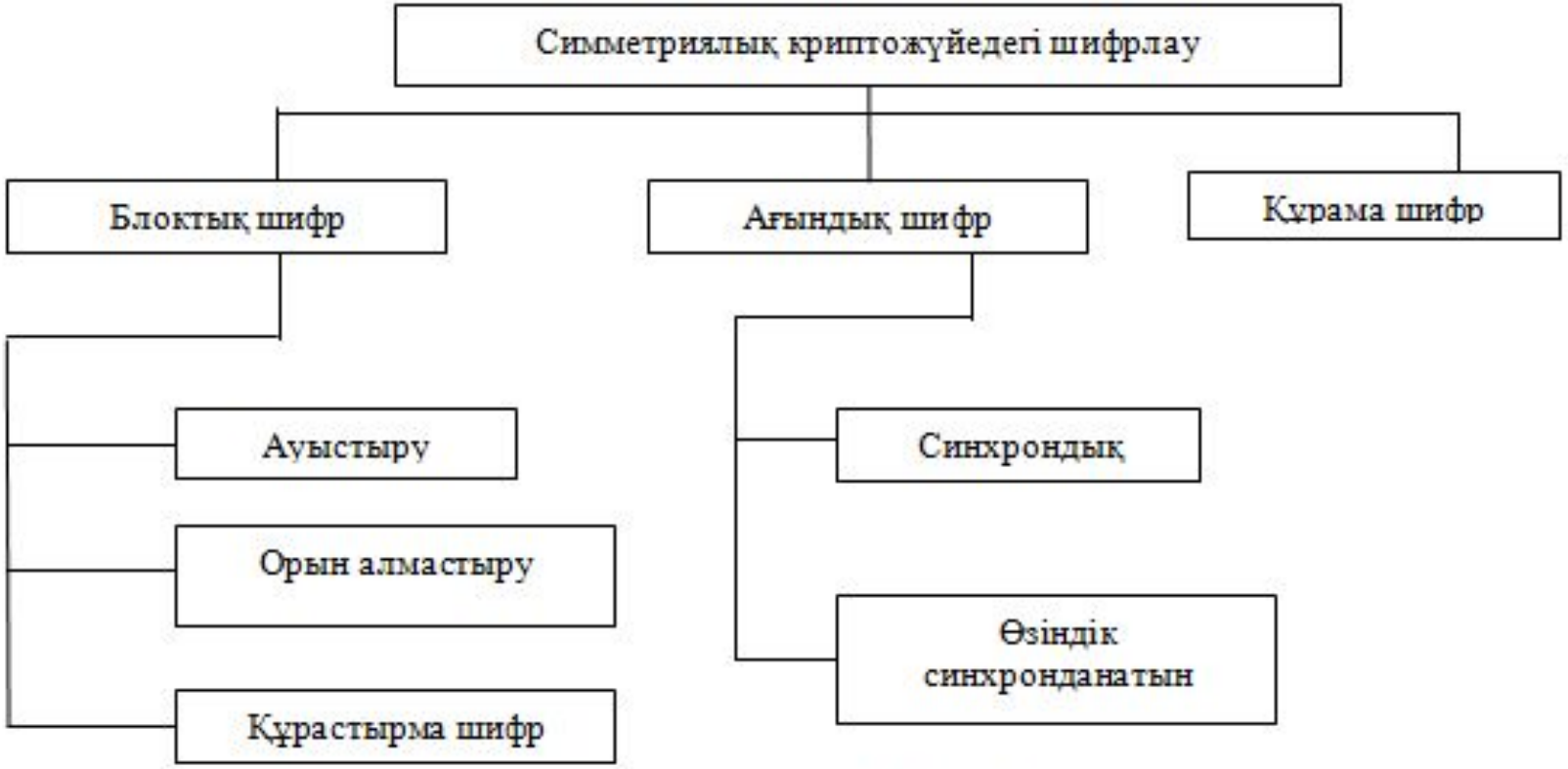
- 7. Шифрлеу процесінде хабарға енгізілетін қосымша биттер шифрленген мәтінде толық және сенімді жасырылуы тиіс.
- 8. Шифрленген мәтіннің ұзындығы бастапқы мәтіннің ұзындығына тең болуы тиіс.
- 9. Шифрлеу процесінде тізбектей қолданылатын кілттер арасында жай және жеңіл орнатылатын тәуелділіктер болмауы керек.
- 10. Мүмкін болатын жиындардың ішіндегі кез келген кілт ақпаратты сенімді қорғауды қамтамасыз етуі тиіс.
- 11. Алгоритм программалық тәрізді аппараттық іске асуды жіберуі тиіс, бұл жағдайда кілт ұзындығының өзгеруі шифрлеу алгоритмінің сапалы төмендеуіне әкелмеуі керек.

Шифрлеу әдістері

- Шифрлеудің екі негізгі әдістерін ерекшелейді:
  - **Симметриялық шифрлеу**, басқаша жабық кілтпен шифрлеу;
  - **Ассиметриялық шифрлеу**, басқаша ашық кілтпен шифрлеу;

Құпия кілтпен шифрлеу

- Симметриялық шифрлеу кезінде шифрлеу және дешифрлеу процесі қандайда бір құпия кілтті пайдаланады.
- Симметриялық шифрлеу кезінде алгоритмнің екі типі қалыптастырылады :
  - Ағындық шифрлеу (бит бойынша)
  - Блокты шифрлеу (шифрлеу кезінде мәтін алдын ала блоктарға бөлінеді, көбінесе 64 биттен кем емес)
  - Құрама шифрлар



1-сурет. Симметриялық криптографиялық жүйелердегі шифрлау тәсілдерінің классификациясы

Құпия кілтпен шифрлеу

- Шифрлерді құрудың келесі жалпы принциптерін ерекшелейді:
  - электронды кодтық кітап (қарапайым алмастыру режимі);
  - шифр блоктарын тізбектеу (кері байланыспен гаммалау режимі);
  - шифрмәтін бойынша кері байланыс;
  - шығару бойынша кері байланыс (гаммалау режимі).

Блоктық шифрлар. Блоктық шифрлау кезінде бастапқы мәтін ұзындығы тұрақты бекітілген блоктарға бөлінеді. Блок мәтіндері бір-біріне қатыссыз бөлек шифрланады. Шифрлау үшін барлық блоктарға бір ғана кілт қолданылады. Шифрлау тәсілдері ауыстыру, алмастыру, құрама шифрлар болып бөлінеді.

Ауыстыру шифры (подстановка)

Ауыстыру шифры белгілі бір ереженің көмегімен бастапқы мәтін символдарын басқа символдармен ауыстыру арқылы анықталады. Егер шифрлау үшін бір әліпби қолданса, онда ол көп әліпбиді немесе полиәліпбилі деп аталады. Бір әліпбиді шифрдің ең қарапайым мысалы Цезарь шифры.

Әліпбидің әрбір символына сан сәйкес қойылсын. Мысалы:

A = 0, B = 1, C = 2, ..., Y = 25

Цезарь хаттарды келесі формуланың көмегімен шифрлаған:

Ciphertext_letter = (plaintext_letter + 3) mod n.

Дешифрлау үшін келесі формуланы қолданған:

Plaintext_letter = (ciphertext_letter - 3) mod n.

Мұндағы *plaintext_letter* – ашық мәтіндегі символға сәйкес сан, c*iphertext_letter* – шифр мәтіндегі символға сәйкес сан, n - әліпбидегі белгілер саны. Қолайлылық үшін біз ағылшын әліпбиін қолданамыз, яғни n = 26.

Цезарь шифрын жалпылауға болады. Келесі формуланың

Ciphertext_letter = (plaintext_letter + 3) mod n.

орнына

Ciphertext_letter = (plaintext_letter + k) mod n формуласын қолданайық. Мұндағы k – шифрлау кілті. Шифрлаудың бұл тәсілі әліпбиді тұрақты позицияға жылжытумен пара пар.

Мысалға «computation» деген түйінді сөз таңдап алайық. Шифр әліпбидің алғашқы символдары ретінде кілт символдарын алады. Қайталанатын символдар әліпбиге бір реттен артық енбеуі тиіс. Келесі символдар алғашқы әліпбиге сәйкес жазылады. Әр символ бір рет қолданылады.

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

c o m p u t a I n b d e f g h j k l r g s v w x y z

Виженер (Vigenere) шифры

Виженер шифрінде d әріптерінен тұратын кілт қолданылады. Мысалы, латын алфавитін пайдаланған кезде

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
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

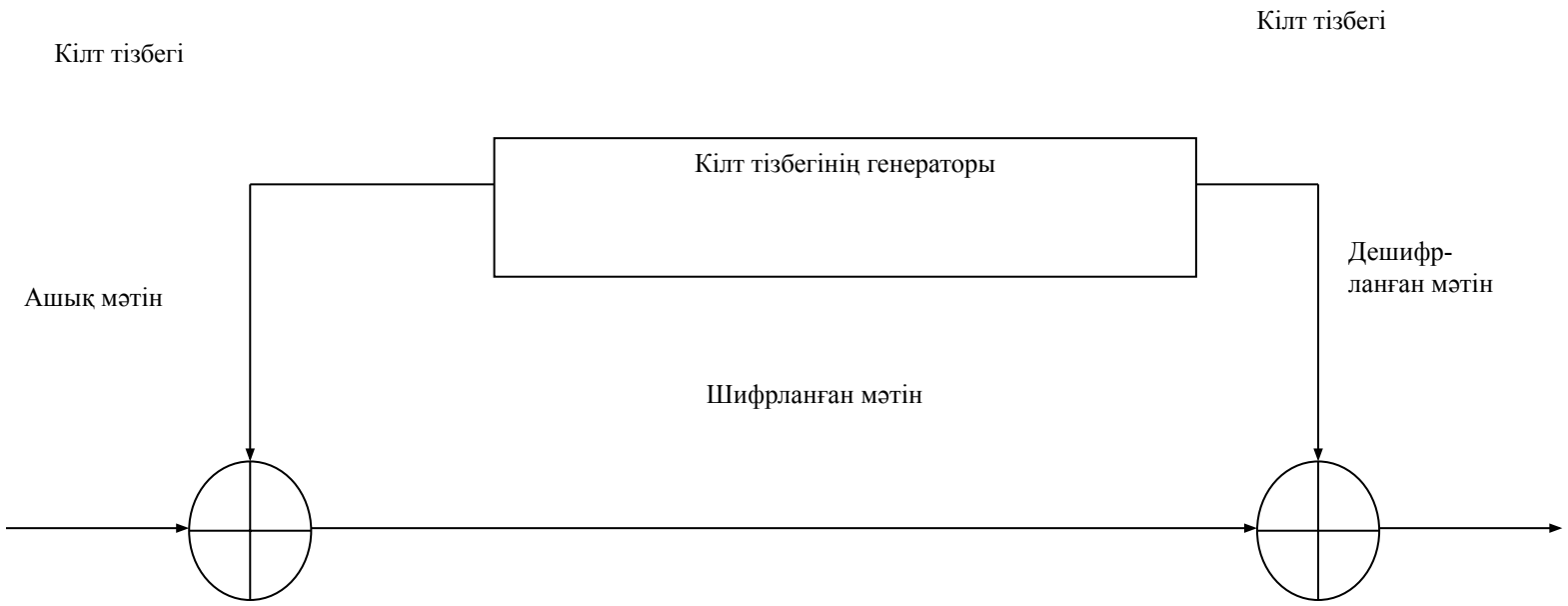
KEY кілті көмегімен THISISATESTMESSAGE хабарламасын түрлендірейік

Исходный текст	THI	SIS	ATE	STM	ESS	AGE
	19,7,8	18,8,18	0,19,4	18,19,12	4,18,18	0,6,4
Ключ	KEY	KEY	KEY	KEY	KEY	KEY
	10,4,24	10,4,24	10,4,24	10,4,24	10,4,24	10,4,24
Зашифрованный текст	3,11,6	2,12,16	10,23,2	2,23,10	14,22,16	10,10.2
	DLG	CMQ	KXC	CXK	OWQ	KKC

Құрастырма шифрлар.

Бұл шифрдың негізінде, сенімді криптожүйе құрастыру үшін ауыстыру және орын алмастыру сияқты қарапайым шифрларды алма – кезек бірнеше рет қолдану идеясы жатыр.
DES, AES және басқа көптеген алгоритмдер шифрдің осы түріне жатады.

Ағындық шифрлар. Егер блоктық шифрлау алгоритмдері мәтінді блоктарға бөліп оларды бір бірден ретімен шифрлайтын болса, ағынды шифрлау алгоритмі мәтінді бөліктемей әр элементін шифрлап ағынды күйде жіберіледі. Шифрлау және дешифрлау негізінен 2 модулі бойынша ашық және кездейсоқ кілт тізбегін қосу операциясын қолданады. Тарихи бірінші ағынды шифр Вернам шифры (6-суреті). Вернам шифрының ерекшелігі оның кілт тізбегінің шифрлауында. Бұл шифрдың практикалық қолданылуы өте ұзын кілт тізбектерінің жасалуына байланысты қолайсыз деп есептелінеді.



Вернам шифрының сүлбесі

- *Синхрондық шифр*. Синхрондық шифрда кілт тізбегі ақпарат ағынына байланыссыз. Хабар алушы және хабар жіберуші жағында кілт тізбегі генераторының жұмысы синхрондалған болу керек. Әйтпесе бір бит мәліметтің жоғалып кетуі қалған символдардың қате дешифрлануына әкеледі.
- *Өзіндік синхронданатын шифр*. Шифрдің бұл түрінде ашық мәтін символдары алдыңғы n символға байланысты шифрланады. Ол алдыңғы n символ кілт тізбегінің жасалуына қатысады. Синхрондау режимі әр n шифрмәтін символынан кейін автоматты түрде орындалады.

Құрама шифрлар. Құрама шифр алгоритмінде блоктық және ағындық шифрлау тәсілдері бірге қолданылады. Практикада құрастырма шифр DES алгоритмінің әр түрлі режимдерінде пайдаланылады.

Идеал шифр талабы. Клод Шеннон егер:

- Біркелкі таралу заңдылығымен шын мәнінде кездейсоқ екілік тізбек болып табылатын кілт қолданса;
- Кілт ұзындығы бастапқы хабардың ұзындығына тең болса;
- Кілт бір ғана рет қолданса шифр абсолют сенімді болады деп дәлелдеді.

Бұл үш талаптың бірден орындалуы әрине қиынға түседі.

Дегенмен абсолют сенімді шифр бар және ол *бір жолғы блокнот* деп аталады (onetime pad). Шифрді 1917 жылы Мэйджер Джозеф Мобори және Гильберт Вернам ойлап тапқан. Кілттің кездейсоқ символдарының тізбегі блокнот беттеріне жазылады. Хабар жіберуші шифрлау үшін кілтті осы блокноттаналып шифрлау процедурасын аяқтағаннан кейін қолданған бетті жояды. Хабар жіберушінің де тура сондай блокты болуы тиіс. Шифрмәтінді дешифрланғаннан кейін ол да қолданған бетті жояды.

Шабуыл

Төменде шабуылдың негізгі түрлерін келтірейік.

Тек шифрмәтін қолданып бұзу (a ciphertext-only attack). Криптоаналитик тек қана бір алгоритммен шифрланған бірнеше шифрмәтінге қатынай алады. Бұзғыштың себебі – кілт ашу немесе бастапқы мәтінді ашу. Шабуылдың бұл түрі ең қиын болып саналады.

Ашық мәтін қолданып бұзу(a known plaintext attack). Криптоаналитик шифрмәтінмен ашық мәтінге қатынай алады. Мақсаты кілт табу. Осы орайда мынадай сауал пайда болуы мүмкін: Мұндай жағдай өмірде туындай алады ма? Шын мәнінде сіз ашық мәтінге қатынай алатындай жағдай көп. Мысалы, сізді қызықтырып отырған адам мәтіні бірдей хабарларды бірнеше адамға жіберу мүмкін (көп адамның бірі – сіз). Шифрмәтіннің бастапқы мәтіні сізге алдын-ала белгілі болуы мүмкін, мысалы, ол абонент резюмесі. Егер бастапқы мәтін сізге түгелдей белгілі болмаса, онда сіз әрқашан оның кейбір бөліктері жайында болжау жасай аласыз. Мысалы, хаттың бастамасы, соңы т.б.

Таңдалған ашық мәтін қолданып бұзу (a known plaintext attak). Алдыңғы шабуыл түріне қарағанда бұл шабуыл күштірек. Криптоаналитик ашық мәтіндерді таңдап қана қоймай олардың сәйкес шифрмәтініне де қатынай алады. Мысалы, сіз құжатты бұзғышқа тәуелді адамнан алып, оны шифрланған күйде басқа біреуге жіберуіңіз мүмкін.

Таңдалған шифрмәтін қолданып бұзу (a chosen ciphertext attack). Толығырақ аты: таңдалған ашық мәтін мен шифрмәтін қолданып бұзу. Криптоаналитик таңдап алған мәтіннің әрқайсысына сәйкес шифрмәтіннің әрқайсысына сәйкес мәтін ала алады. Кілт табуы керек.

Таңдалған кілт қолданып бұзу (a chosen key attack). Практикада крипожүйелер бірнеше шифрлау алгоритмдерін қолданады. Шифрлау үшін керекті кілттер бастапқы кілттен есептелінеді. Әрине бұзғыш, кілтті білмейді және таңдай алмайды. Ол алгоритмде қолданылатын бірнеше кілттің арасындағы байланысты зерттейді. Шабуылдың бұл түрі блоктық шифр бұзу үшін пайдалы болуы мүмкін.

«Туған күндер» шабуылы (Birthday attack). Математикалық статистикада стандартты «туған күндер» парадоксы белгілі. Егер бөлмеде 23 адам болса, онда олардың ішінде туған күні бірдей екі адамның табылуы ықтималдығы 50 % артық. «Туған күндер» шабуылы мәндері бірдей элементтерді табуға негізделген. Мұндай элементтер «коллизия» деп аталады. Әр элемент N мән қабылдай алсын. Алғашқы коллизияны сіз шамамен $\sqrt{N}$ кездейсоқ мәндерді қарастырғаннан кейін күтуіңізге болады. Расында, егер N мүмкін элементтің ішінен m элемент таңдалса, олар $m(m-1)/2$ жұп құрайды. Коллизия табу ықтималдығы $m(m-1)/2N$ санына жақын. $m \approx \sqrt{N}$ деп таңдасақ бұл ықтималдық шамамен 50% құрайтынын көреміз.

Мысал. Қаржылық транзакция кезінде аутентификация үшін тұтынушы 64 биттік кілт қолдансын. Онда 264 мүмкін кілт бар, алайда бұзғыш алғашқы коллизиясын 232 транзакциясын қарастырғаннан кейін табуы ықтимал. Аутентификация мезетінде бұзғыш кілт мәндерін емес, h(k, m) мәндерін алады, мұндағы k – кілт, m – хабар, h – хэш функция. Әр транзакция үшін m белгілі болсын. h(k, m) мәнін MAC (message authentication code) деп атайды.

«Ортада кездесу» шабуылы (Meet-in-th-Middle attack). Бұл шабуыл «Туған күндер» шабуылының модификациясы болып табылады. Алдындағы мысалға оралайық. Бұзғыш алдын ала кездейсоқ 2^{32} 64 битті кілттер таңдайды. Әрбір кілт үшін олардың MAC мәндерін есептеп, кілт мәндерімен бірге сақтап қояды. Енді 2^{32} транзакциясын жасырын тыңдап, олардың MAC мәндерін салыстырады. Өзінің мәліметтер базасындағы MAC мәні кездескен мезетте ол әрекетін тоқтатады. Мәліметтер базасында MAC мәніне сәйкес кілт мәні жазылғандықтан енді ол жалған кілтпен аутентификация процесін өтеді. Жұмыс көлемі 2^{32}, мұндағы 2^{32} – алдын-ала орындалатын есептеулер үшін және 2^{32} жасырын таңдау үшін. «Туған күндер шабуылы» мен «Ортада кездесу» шабуылдарының айырмашылығы «Туған күндер» шабуылында бұзғыш таңдап алынған жалғыз мән үшін қайталануды күтеді, ал «ортада кездесу» шабуылында бұзғыш екі жиынның қиылысу нүктесін іздейді. Бірінші жиын – бұзғыш таңдап алған кездейсоқ кілттер, екіншісі – жасырын таңдау кезіндегі табылған мәндер. «Ортада кездесу» шабуылы «туған күндер» шабуылына қарағанда күштірек.