Лекция №14. **Қорғау механизмдары сенімділігіне баға беру Компьютерлік жүйелердің қауіпсіздігі.**

Қорғау сенімділігіне баға беру принциптері.

Жергілікті желілерді қорғау.

Жеке ақпаратты қорғау бағдарламалық құралдары

Қорғанушылықты талдау

- Қорғанушылықты талдау барлық желінің әлсіз орындарын іздеу негізінде жүзеге асады.
- Желі қосуларынан, түйіндерінен (мысалы, коммуникациялық жабдықтардан), хосттардан, жұмысшы станциялардан, қосымшалардан және деректер базаларынан құрылған.
- Бұл элементтер олардың қорғау тиімділігін бағалауға және олардағы белгісіз осал тұстарын іздеуде мұқтаж болады.
- Қорғанушылықты талдау процесі желінің “әлсіз орындарын” табуға арналған зерттеуді болжайды және алынған мәліметтерді жалпылау, соның ішінде есептілік түрінде.
- Егер осы технологияны іске асырушы жүйеде бейімделетін компонент болса, онда табылған осалдылықты жою автоматты түрде жүзеге асады.

Қорғанушылықты талдау жағдайында әдетте сәйкестендіреліді:

- жүйелердегі «люктар» (back door) және «троян аты» сияқты бағдарламалары;
- әлсіз парольдер;
- сыртқы жүйелерден енуге сезінушілігі және «қызмет етуден бас тарту» типті шабуылдарына;
- ОЖ қажетті жаңартуларының жоқ болуы (patch, hotfix);
- Web - серверлердің және ДБ жүйе аралық экрандарының дұрыс емес күйге келтіруі.
- неправильная настройка межсетевых экранов, Web-серверов и БД.

Қорғау құралдары

- Қорғау құралдары желілік деңгейде (network-based), операциялық жүйе деңгейінде (host-based) және қосымша деңгейінде (application-based) жұмыс жасай алады.
- Ең кең таралған желілік сервистерді және протоколдарды қорғанушылығын талдау құралдары.
- Бұл, ең алдымен, қолданылатын протоколдардың әмбебаптығымен байланысты.
- IP, TCP, HTTP, FTP, SMTP протоколдарының үйреншіктілігі және жаппай қолдануы осы желілік ортада жұмыс істеуші ақпараттық жүйенің қорғанушылығын жоғары тиімділік дәрежесімен тексеруге мүмкіндік береді
- Екінші көп таралған құралдар – ОЖ қорғанушылық қабілетін талдау. Бұл бірсыпыра операциялық жүйелердің әмбебаптығымен және көп таралғандығымен байланысты (мысалы, UNIX и Windows XP).

Осалдылықты тексеретін негізгі екі механизм

- Осалдылықты тексеретін негізгі екі механизмы бар - *сканерлеу (scan)* және *зондпен тексеру* (probe).
- *Сканерлеу* - енжар талдау механизмы, мұның арқасында сканер осалдылық бар екендігін анықтауға тырысады оның нақты растаусыз - жанама белгілері бойынша.
- Мынау әдіс орындауға ең жылдам және қарапайым келеді.
- Бұл әдіс "логикалық шығару" (inference) деп ататалады.

Сканерлеу

- мынау процес сканерлеу жағдайында табылған әрбір портты ашық порттарды сәйкестендіреліді, әрбір желілік құрылғыда табылған және порттармен байланысты тақырыптарды жинайды (banner),
- Әрбір алынған тақырыбы желілік құрылғылардың, операциялық жүйелердің және потенциалды осалдылықтардың анықтау ережелері кестесімен салыстырылады.
- Өткізілген салыстыру негізінде осалдылық бар немесе жоқ туралы қорытынды шығаралыда

Зондпен тексеру

- *Зондпен тексеру* - белсенді талдау механизмы, талданатын түйінде осалдылық бар немесе жоқ екендігіне көз жеткізіуге мүмкіндік береді.
- Зондпен тексеру осалдылықты тексеруге қолданылатын шабуылды имитациялау (еліктеулері) жолымен атқарылады,.
- Мынау әдіс "сканерлеу“ қарағанда көбірек баяу, бірақ әрқашан одан анағұрлым көбірек дәлірек.

"растау" (verification)

- ISS компаниясы терминдерінде осы әдіс "растау" (verification) аттын алды
- Cisco компаниясына сәйкес процес сканерлеу (“логикалық шығару") барысында алынған ақпаратты қолданады, әрбір желілік құрылғыны толық талдауға арналған.
- Мынау процес сонымен қатар шабуылдарды орындау белгілі әдістерін, осалдылықтың шамаланған толық растау үшін және басқа енжар әдістерімен табылмайтын осалдылықты анықтауға қолданады мысалы, "қызмет етуден бас тарту" ("denial of service") шабуылдарын.

Аталған механиздер іс жүзінде келесі әдістермен атқарылады

- ***"Проверка заголовков" (banner check) -*** ряд проверок типа "сканирование", позволяющий делать вывод об уязвимости, опираясь на информацию в заголовке ответа на запрос сканера
- ***"Активные зондирующие проверки" (active probing check) -*** основаны на сравнении "цифрового слепка" (fingerprint) фрагмента программного обеспечения со слепком известной уязвимости (антивирусные системы)
- ***"Имитация атак" (exploit check)*** - данные проверки относятся к механизму "зондирования" и основаны на эксплуатации различных дефектов в программном обеспечении.
- Некоторые уязвимости не обнаруживают себя, пока вы не "подтолкнете" их. Для этого против подозрительного сервиса или узла запускаются реальные атаки

Сканерлеу кезеңдері

- **Сбор информации о сети**. На данном этапе идентифицируются все активные устройства в сети и определяются запущенные на них сервисы и демоны. На уровне ОС данный этап пропускается
- **Обнаружение потенциальных уязвимостей**. Сканер использует описанную выше базу данных для сравнения собранных данных с известными уязвимостями при помощи проверки заголовков или активных зондирующих проверок
- **Подтверждение выбранных уязвимостей**. Сканер использует специальные методы и моделирует (имитирует) определенные атаки для подтверждения факта наличия уязвимостей на выбранных узлах сети
- **Генерация отчетов**. На основе собранной информации система анализа защищенности создает отчеты, описывающие обнаруженные уязвимости
- **Автоматическое устранение уязвимостей**. Этот этап очень редко реализуется в сетевых сканерах, но широко применяется в системных сканерах (например, System Scanner)

Internet Security Systems (ISS) компаниясы шешімдері

- В комплект ПО SAFE suite Enterprise входят:
  - система анализа защищенности на уровне сети Internet Scanner
  - средство анализа защищенности на уровне хоста System Scanner
  - система анализа защищенности на уровне баз данных Database Scanner
  - система обнаружения сетевых атак Real Secure
  - система принятия решений SAFE suite Decisions

Ақпараттық қауіпсіздікті қамтамасыз етуіндегі Microsoft өнімдері және технологиялары

Криптографиялық жүйелер

Мақсаттары

- Криптографиялық алгоритмдердің негізгі түрлерін қарап шығу
- Асимметриялық және симметриялық шифрлаудың артықшылықтарны және кемшіліктерін салыстыру
- Криптографияның қолдану облысын зерттеу
- Шифрлау алгоритмдерін қолдануын регламенттейтін стандарттармен танысу

Эпиграф

Жасыра білу –
ол корольдардың
ғылымы.

Арман дю Плесси,
кардинал Ришелье

Криптология

- Криптология - екі бағытты қамтитын білім аясы:
  - *криптография –* ақпаратты заңсыз қолданушылардан қорғау мақсатында оны өзгерту әдістері (шифрлау) туралы ғылым
  - *криптоанализ* - шифрларды ашу әдістері және тәсілдері туралы ғылым (және оны қолдану тәжірибесі)

Криптографияның қолдану облыстары

Криптографиялық алгоритмдер

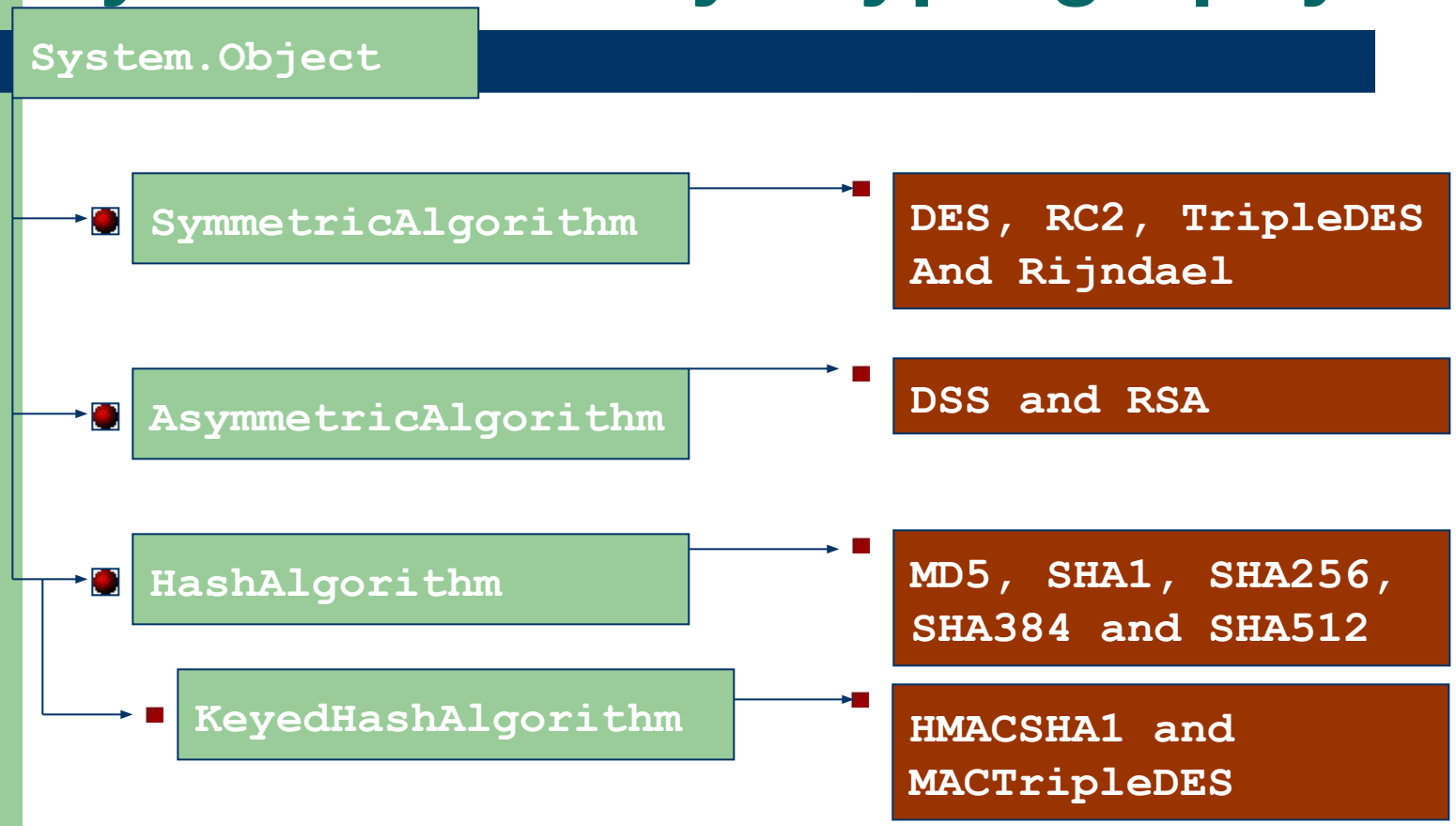
- симметриялық алгоритмдер
- ассиметриялық алгоритмдер
- деректердің хешін алу алгоритмдері
- электрондық қол қоюды алу алгоритмдері

Плюстері және минустері

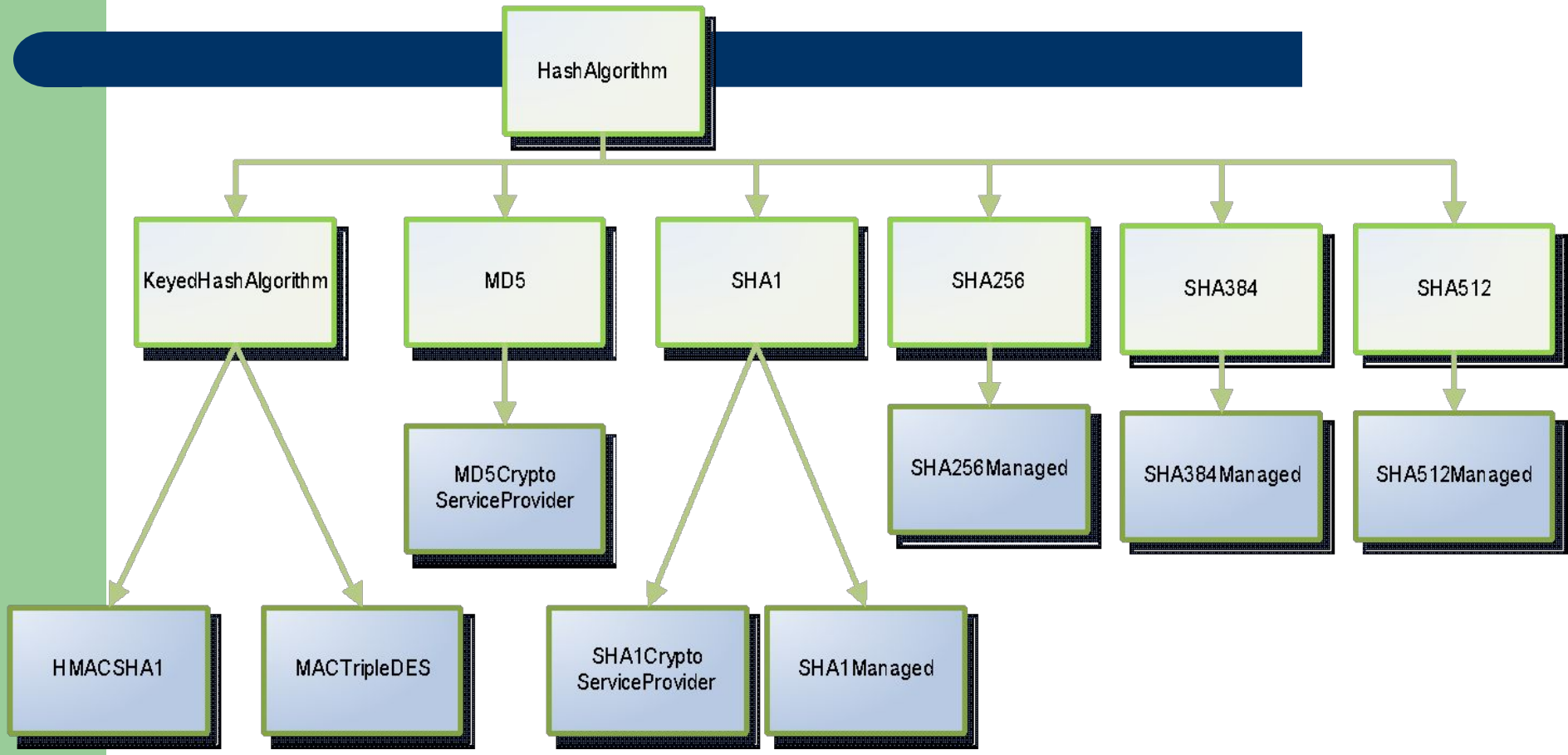
- Симметриялық алгоритмдер
  - жылдамдық, тиімділік, ептеген қосымша шығындар
  - кілттердің айырбас мәселесі
- Асимметриялық алгоритмдер
  - күрделілік, есептеу шығындары
  - кілттермен тиімді айырбас

Екі әдістердің комбинациясы қолданылады

System.Security.Cryptography



.NET-те хеш алу кластар иерархиясы

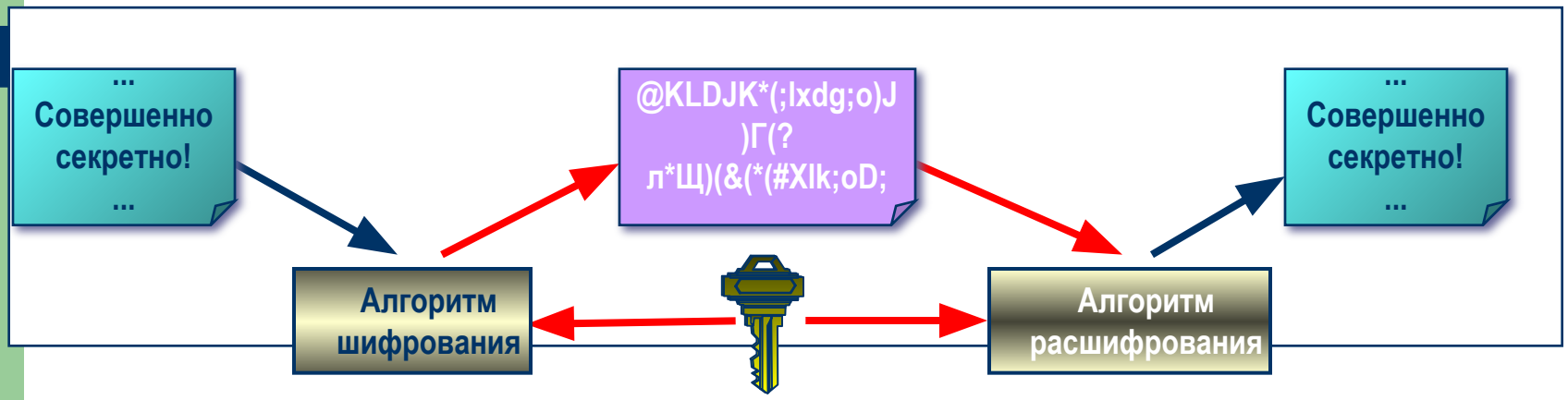


Кілттің ұзындығы

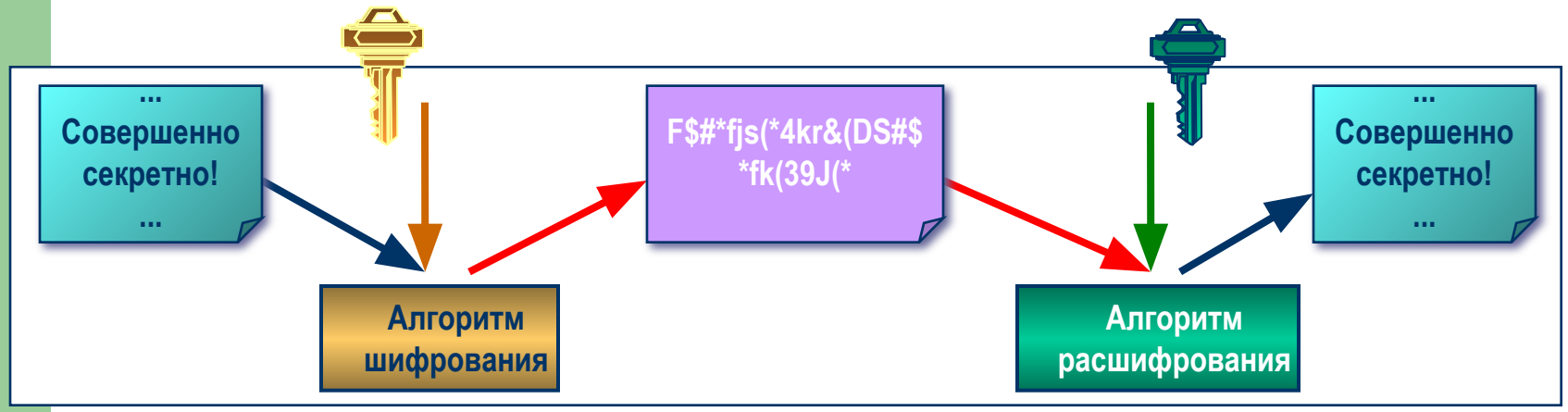
Алгоритм	Возможный размер ключа	Размер ключа по умолчанию
DES	64 bit	64 bit
RC2	40 to 128 bit	128 bit
Triple-DES	128, 192 bit	192 bit
Rijndael	128, 192, 256 bit	256 bit

Шифрлау әдістері

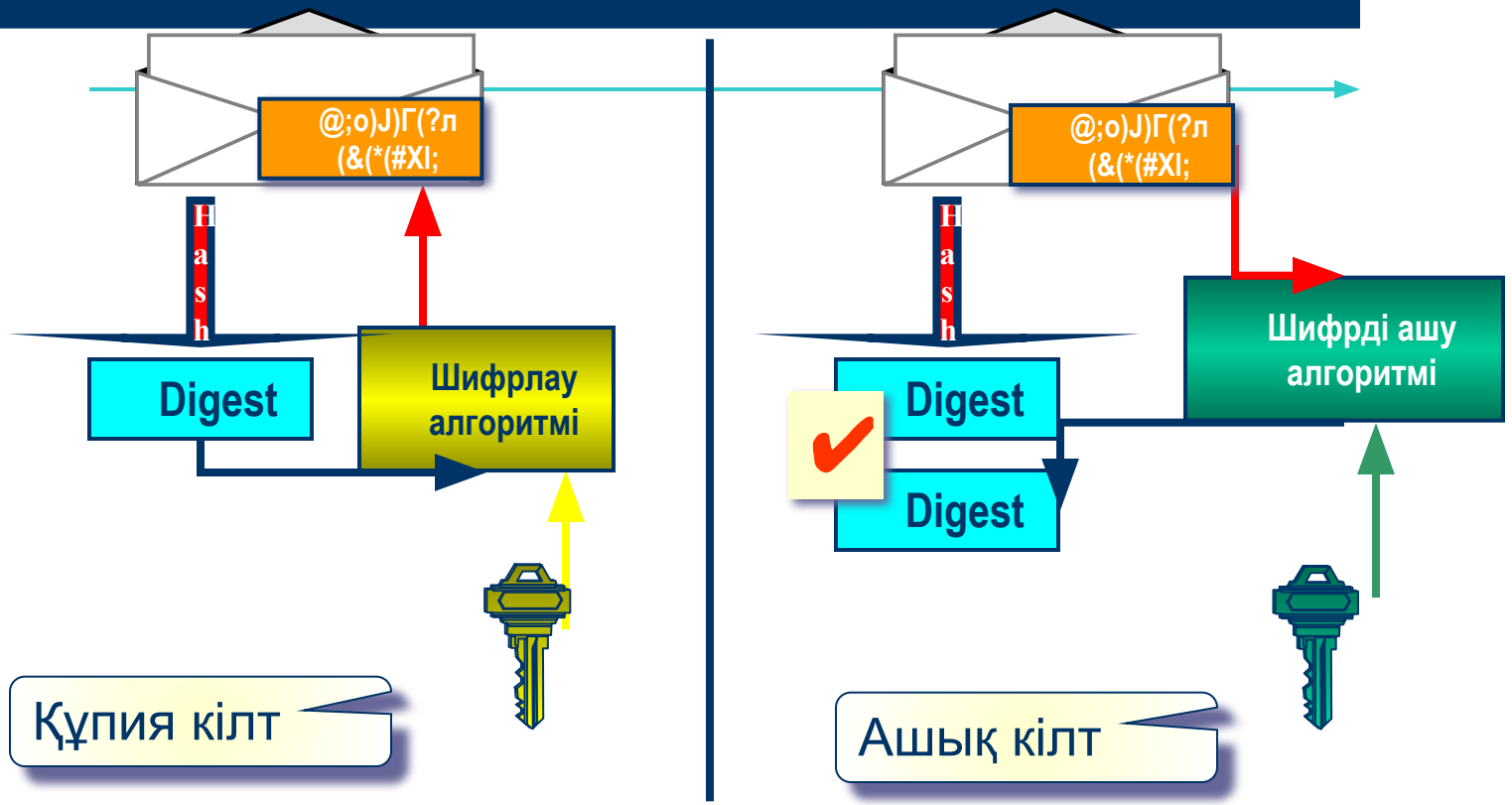
Симметриялық шифрлау – бір кілт



Асимметриялық шифрлау –кілтер жұбы: ашық және құпия



Электронды - цифрлық қол қою



Симметриялық шифрлау

- Категориялар
  - блоктық шифрлар
  - тасқынды шифрлар
- Шеннон ұсынған қарапайым криптографиялық өрнектеулерді қолдану арқылы көп рет шифрлау қағидасы
  - алмастыру
  - ауыстыру
- Өрнектеулерді іске асыратын түйіндер
  - ***P-блоки*** (*P-box, permutation box*)
  - ***S-блоки*** (*S-box, substitution box*)

Стандарттар

ГОСТ 28147-89

- Ресми аталуы: «Криптографиялық өрнектеу алгоритмі ГОСТ 28147-89».
- 1989 жылы КСРО –да қабылданды.
- Блокті шифр, Фейстел схемасы бойынша құрылған шифрлеудің 32 циклі.
- Ақпараттық блоктың ұзындығы – 64 бита
- Кілттің ұзындығы– 256 бит

- *AES (Rijndael)*
  - 2001 жылы АҚШ-та қабылданды.
  - Итерациялық блокты шифр, «Квадрат»
  - архитектурасы бар
  - Кілттің ұзындығы: 128, 192 или 256 бит
  - Блоктың ұзындығы: 128, 192 или 256 бит

Microsoft қолдануға ұсынбайды:

- DES / 3DES
- IDEA
- RC2 и RC5
- Blowfish / Twofish
- CAST

Асимметриялық криптожүйелер

- Рюкзактық криптожүйе (Knapsack Cryptosystem)
- RSA криптожүйесі
- Эль-Гамаля криптожүйесі – EGCS (El Gamal Cryptosystem)
- Эллиптикалық қисықтар қасиеттеріне негізделген криптожүйе – ECCS (Elliptic Curve Cryptosystems)

Асимметриялық криптожүйелер мүмкіндік береді:

- Алдын ала кілттердің ауысуы үшін құпия каналдардан арылуға
- Математикалық есептерді шешуде шифрді бұзу орнына, яғни соңында, криптожүйенің төзімділігін қарастырады
- Криптография есептерін шешу шифрлеуден ерекше, мысалы электронды іс-қағаздардың құқықтық қамсыздандыру мәселесін шешуге болады.

ЭЦП схемасы қосады:

- қол қою алгоритмы
- қол қоюды тексеру алгоритмы
- қол қою және оның тексеру үшін кілттер жұбын генерациялау алг

Стандарттар

- 2001 ж дейін.:
  - *Рессей*: ГОСТ Р34.10-94. Ақпараттық технология. Ақпаратты криптографиялық қорғау. Электронды-цифрлік тексеру кезінде ассиметриялық криптографиялық алгоритм деректері негізінде өңдеу процедуралары.
  - АҚШ: FIPS PUB 186. Digital Signature Standard (DSS).
- 2001 ж кейін. –эллиптикашлық қисықтарға ауыстыоылған:
  - *Рессей*: ГОСТ Р34.10-01. Ақпараттық технология. Ақпаратты криптографиялық қорғау.Электронды цифрлық жазуларды тексеру , құрылу

  АҚШ: FIPS PUB 186-2. Digital Signature Standard (DSS)

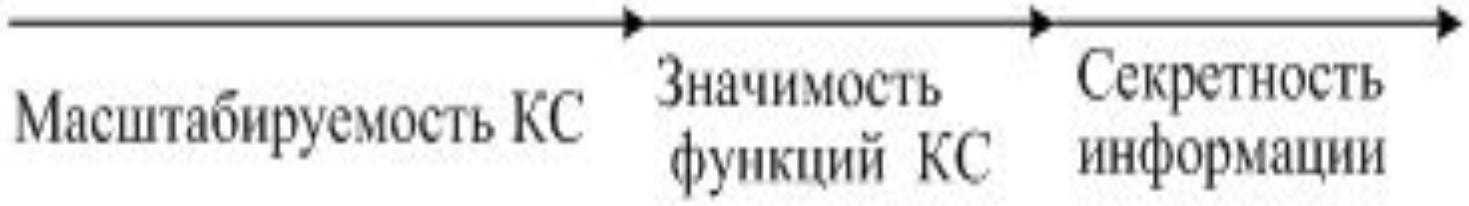
Криптографияны на Windows XP/Server 2003 қолдану туралы ұсыныстар

- AES-128 (AES-192, және AES-256)
- RSA 2048 (немесе одан да ұзақ кілттермен)
- SHA-2 (т.е. SHA-256 және SHA-512)
- DSA (SHA-2/RSA)

Криптографияны қолдану бойынша ұсыныстар Windows Vista/7/Server 2008

- AES (шифрлау)
- EC-DSA (электронды-цифрлық қол қою)
- EC-DH или EC-MQV (құпия кодтармен алмасу)
- SHA-2 (хештеу)

Нақты компьютерлік желідегі ақпаратты қорғау жүйесінің ролін анықтаушы қосынды вектор



- Основными факторами, объективно влияющими на увеличение удельного веса систем защиты в современных КС, являются:
  - расширение функций, повышение значимости и масштабов КС с одной стороны
  - постоянное появление новых угроз безопасности и их источников - с другой

Роль систем защиты информации в процессе функционирования КС

- Несмотря на постоянный рост внимания к проблемам защиты информации, процесс создания безопасных ИТ идет весьма неравномерно.
- Этому способствует двойственность природы СЗИ:
- С одной стороны они являются неотъемлемой функциональной частью КС,
- а с другой - внешним барьером между КС и угрозами ее безопасности.

Қорытынды

- Неизбежно участвуя во всех значимых процессах, происходящих в КС, но выполняя функции, не связанные с их прямым назначением, а зачастую противоположные ему, СЗИ, как правило, снижают эффективность КС и существенно удорожают их создание и эксплуатацию
- Лавинообразное развитие ИТ без системной проработки направлений обеспечения безопасности приводит зачастую к торможению их практического использования и излишним затратам на защитные надстройки
- США более 50 учреждений 75 млрд. долларов ежегодно тратятся на информационную безопасность

Тест сұрақтары

261. Ашық кілтті крифтографиялық жүйелерде қолданады
262. Элъ-Гамаль жүйесі күрделілікке негізделген
263. RSA криптожүйесі негізіндегі күрделілік
264. Мак-Элиса криптожүйесі қолданады
265. Қатал математикалық басқа криптоанализдың әдістері дәлелдемеген
266. Қасиет ие болатын таратуларды бағдарламалар және АЖ репликациясы
267. Компьютер вирустері мекендеулер орта бойынша жіктеледі
268. Компьютер вирустері мекендеуді ортаның жұқтырулары әдіс бойынша жіктеледі
269. Деструкциялы (зиянкестік) әсерлердің қауіп-қатерінің дәрежелері бойынша бөлуге болады
270. Компьютер вирустері жұмыс жасаулар алгоритм бойынша бөлуге болады

Тест сұрақтары

271. Әсердің тетігі атқарылатын файлдардың көшірмелерінің жасауында тұрады
272. Басқа желінің абоненттеріне тарату мекенжайларды есептейді және берілуін жүзеге асырады
273. Файлдарға БЖдың үндеулерді ұстап қалуы мекендеуді ортадағы өз қатысуы жолымен маскировка жасайды
274. Пайдалы бағдарламалар, және олар жүкте қолданушыларын алдап сендіретінін көрінеді
275. Тұрақты айрықша топтары болмайтын вирустар сигнатуралар
276. "Ортақ белгілер" қауіпсіздік талаптарының иерархиясы енгізілген
277. Жұртқа белгілі, талаптардың "пәндік" топтауын анықтайды
278. Сынып шектеріндегі талаптардың қаталдық тағы басқа реңктері бойынша өзгешеленеді
279. Дараланатын табандатқан талаптардың ең төменгі жиыны
280. Бөлінбейтін қауіпсіздік талабы