ОҚУ ПӘНІНІҢ ТАҚЫРЫПТАРЫ БОЙЫНША ДӘРІС ТЕЗИСТЕРІ

№1 дәріс. **Пәнге кіріспе. Терминоглогия. Криптографиялық шифрлер. Криптоталдау**

Мақсаты: Курстың мазмұны мен міндетін анықтау, компьютерге дейінгі шифрлерді криптоталдау әдістерін қарастыру

Дәріс жоспары:

- Кіріспе. Криптоталдау мен критпографияның негізгі түсініктері
- Криптоталдау шабуылдары мен әдістері
- Криптографиялық алгоритмдердің классификациясы
- Ауыстыру және өзгерту шифлері. Моно және көпалфавитті ауыстыру
- Дешифрлеу әдістері. Көпалфавитті жүйелерді талдау әдістері.Дешифрлеу әдістерінің классификациясы
- Керкхофф ережесі
- Шеннон бойынша толық құпиялылық
- Шифрлеу алгоритмдерінің күрделілігі
- Заманауи алгоритмдерді криптоталдау нәтижелерінің жобасы

Компьютерлер пайда болғанға дейін криптография текстік алгоритмдерге негізделді. Бұл алгоритмдерде символдарды ауыстыру, олардың орындарын өзара алмастыру немесе осы екі әдістерді бірге қолдану амалдары текстің әрбір символы үшін қолданылады.
Қазіргі шифрлар символдармен емес, биттермен жұмыс істейді. Олардың көпшілігі ауыстыруды және орындарды өзара алмастыруды жасайды:

Компьютерге дейінгі криптография	**Компьютерлік криптография**
Текстік алгоритмдер	Информация биттері

Төменде классикалық деп аталатын шифрлердің негізгі түрлері және олардың мысалдары келтірілген.

<table>
<tr><th colspan="2">Компьютерге дейінгі/классикалық/текстік (ағындық) шифрлар</th></tr>
<tr><td>Ауыстыру
Ауыстыру шифры – ашық текстің әрбір символын басқа символға ауыстыру арқылы шифртекст жасайтын шифр</td><td>Орын ауыстыру
Ашық текст өзгермейді, тек оның символдары орындарын өзгертеді
Мысал. Тігінен орын ауыстыру қарапайым шифрі</td></tr>
<tr><td>1. Жай ауыстыру шифрі (жай айырбастау шифрі, моноалфавиттік шифр)
Ашық текстің әрбір символын шифртекстің сәйкес символына ауыстыратын шифр
Мысал. Аддитивтік шифр (Цезарь шифрі), ROT13 программасы</td><td rowspan="3">Шифрді нығайту үшін шифртекстке орын ауыстыру шифрін қолдануға болады.

Ауыстыру шифріне қарағанда сирегірек қолданылады, себебі жады мөлшерін көп қажет етеді, ал кейбір жағдайда өлшемі қатаң бекітілген хабарламаларды талап етеді</td></tr>
<tr><td>2. Омофониялық ауыстыру шифрі
1-ші типті шифрлерге ұқсайды, бірақ ашық текстің бір символына шифртекстің бір немесе бірнеше символы сәйкес келуі мүмкін
Мысалдар. Төмендгі тапсырманы қара</td></tr>
<tr><td>3. Полиграмдық (n-грамдық) ауыстыру шифрі
Символдар блоктарын топтап шифрлайтын шифр
Мысалдар. Playfair, Хилл шифрлары, Хаффман коды</td></tr>
</table>

4. Полиалфавиттік ауыстыру шифры (1568) Бірнеше қарапайым ауыстыру шифрларынан тұратын шифр **Шифр периоды** (кілт ұзындығы) түсінігі **Мысалдар.** Виженер шифры, Бофор шифры, жүгіргіш кілтті шифр (кітап шифры)	
Орын ауыстыру және ауыстыру шифрларының комбинациялары да кездеседі	

Криптоанализдың негізгі қағидасы – Керкхофс ережесі, 19 ғ.: қауіпсіздік тек қана кілттен тәуелді, шифрлау алгоритмінің толық сипаттамасы мен жүзеге асырылуы криптоталдаушыға белгілі.

Көп жағдайда криптоанализ деп кілтті анықтау саналады; криптоанализға криптографиялық алгоритмдер мен протоколдырдың осалдықтарын анықтау әдістерін де жатқызады.

Алгоритмдерді бұзу күрделілігінің классификациясы (Ларс Кнудсен)

4. Толық бұзу. Криптоталдаушы кілтті табады: Dk(C)=P.
3. Глобалдық дедукция. Криптоталдаушы k кілтсіз Dk(C)=P теңдеуіне эквивалентті нәтиже қамтамасыз ететін альтернативті А алгоритмін табады.
2. Кездейсоқ (ішінара) дедукция. Криптоталдаушы қолға түскен криптограмманың ашық текстін табады.
1. Информациялық дедукция. Криптоталдаушы кілт немесе ашық текст туралы кейбір информацияны табады.

Бастапқыда криптоанализ әдістері табиғи мәтіннің лингвистикалық заңдылықтарына негізделіп, тек қарындаш пен қағаз көмегімен жүзеге асырылды. Кейбір бұзу әдістері бірнеше ғасырлар бұрын ойлап табылды. Криптоанализ туралы алғашқы белгілі жазбаша ескерту араб ғалымы Әл-Кинди 9 ғасырда жазған "Криптографиялық хабарламаларды дешифрлеу туралы манускрипт" болып табылады. Бұл ғылыми еңбекте жиіліктік талдау әдісінің сипаттамасы бар. Жиіліктік талдау — классикалық орын ауыстыру немесе ауыстыру шифрларының көпшілігін бұзуға арналған негізгі құрал. XV-XVI ғасырлар кезеңінде Еуропада полиалфавиттік алмастыру шифрлары құрылды және дамыды. Ең танымал шифрлердің бірі — француз дипломаты Блез де Виженердің шифры, оның негізіне әр түрлі жылжыту мәндерімен алынған Цезарьдың бірнеше шифрларын біртіндеп пайдалану жатады. Үш ғасыр бойы Виженердің шифры 1863 жылы Фридрих Касиски осы шифрды бұзу әдістемесін ұсынғанға дейін криптографиялық тұрақты болып саналды.

Уақыт өте келе криптоанализде таза математикалық әдістердің рөлі арта түсуде, оларды іске асыру үшін мамандандырылған компьютерлер қолданылады.

Бақылау сұрақтары мен тапсырмалар

1) Классикалық шифрлардың жіктелуін беру, мысалдар келтіру
2) Криптоанализге және оның міндеттеріне анықтама беру. Ларс Кнудсеннің жіктелуін келтіру
3) Классикалық шифрлардың криптоанализінің тарихы, қазіргі жағдай
4) Керкхофф ережесінің мәні неде?
5) Неміс "Энигма"шифрлау машинасында шифрлаудың қандай түрі қолданылды?
6) Қазақ тіліндегі мәтіндерді шифрлау үшін ROT13 бағдарламасының аналогын жасау. Бағдарламаға қандай атау беруге болады?

7) Қандай да бір тіл (орыс немесе қазақ) үшін омофондық ауыстыру шифрын ұсыну. Бұл шифр үшін ашық мәтін негізінде криптошабуыл жасау. Сипаттама беру, есеп беру
Әдебиеттер: [1, 4] – нег., [4] – қос.

№ 2 дәріс. **Симметриялық шифрлеу**. **Криптобериктік сұрақтары**
Мақсаты: Симметриялық шифрлеу принциптерін, оларды ақпаратты қорғау үшін қолдану, сонымен қатар олардың крипто төзімділігі мәселелерін зерттеу
Дәріс жоспары:
- Классикалық шифрлер (Цезарь, Виженер, Вернам шифрлары)
- Симметриялық блоктық шифрлер. Блоктық симметриялық шифрлеудің принциптері. XOR, жалпы сұлбасы, алгоритмдер параметрлері
Шеннон идеялары. Фейстель желілерін қолданатын және қолданбайтын шифрлар
- Блоктық симметриялық шифрлау алгоритмдері
- Симметриялық ағындық шифрлау (классикалық шифрлар, RC4, A5/1)
- Ағынның синхронды және синхронды емес шифрлары және блоктық шифрлерді шифрлеу режимдері
- Есептеу күрделілігінің теориясы

Төмендегі кестеде симметриялық алгоритмдердің сипаттамасы, жалпы белгілері, мысалдар берілген.

Симметриялық алгоритмдер		
Шешілетін мәселелер: құпиялылықты қамтамасыз ету		
Ақпаратты қалай жасырады: орын ауыстырулар, ауыстырулар		
	Ағындық	**Блоктық**
Классикалық (текстік)	Заманауи компьютерлік, ашық текстті биттер/байттар бойынша өңдейтін	Заманауи компьютерлік, ашық текстті блоктар бойынша өңдейтін. Көбінесе блок өлшемі 64 бит
	РСЛОС-қа негізделген (сызықтық кері байланысы бар жылжыту регистрі)/ ОСӨЖ-ға негізделген (орын ауыстыру бойынша кері байланыспен жылжыту регистрлері)/Басқа тәсілдерді пайдалана отырып	Файстель желісіне негізделген/Файстель желісін пайдаланбайтын
	Мысалдар	
	RC4, SEAL, WAKE, A5, Hughes, XPD/KPD, XOR, Nanoteq, Rambutan, PKZIP	DES, AES, ГОСТ 28147-89, 3DES, RC2, RC5, Blowfish, Twofish, NUSH, IDEA, CAST

Файстель желісі (Файстель құрылымы) — блоктық шифрларды құру әдістерінің бірі. Желі Файстель ұяшығы деп аталатын бірнеше рет қайталанатын (итерацияланған) құрылым болып табылады. Бір ұяшықтан екіншісіне өту кезінде кілт өзгереді, ал кілтті таңдау нақты алгоритмге (Википедиядан) байланысты.

Алгоритмнің есептеу күрделілігі оның уақыт τ және сыйымдылық S күрделіліктері арқылы кіріс мәліметтерінің n мөлшеріне байланысты өлшенеді. **Уақыттық күрделілік** – есеп өлшемінің немесе кіріс деректерінің мөлшерінің функциясы ретінде қарастырылатын тапсырманы алгоритммен шешуге жұмсалатын уақыт. Сиымдылықтық күрделілік – қажетті

машина жадының сиымдылығы. Есеп өлшемінің ұлғаю шегіндегі осы күрделіліктердің беталысы асимптотикалық күрделіліктер деп аталады. Алгоритмнің бұл күрделіліктері осы алгоритмнің көмегімен шешуге болатын есептің өлшемін анықтайды. Күрделіліктер ең жаман және орташа жағдайдағы күрделілік болып екі түрге бөлінеді.

Күрделіліктің басқа да өлшемдері бар: кездейсоқ биттер саны, байланыс арнасының ені, деректер көлемі және т. б.

Алгоритм үшін **n-өлшемді бастапқы деректердің жиынын** әлдебір позициялық санау жүйесінде ұзындығы **n**-нен аспайтын жазба түрінде бейнелеуге болатын сандар жиыны ретінде түсінуге болады.

Алгоритмнің есептеу күрделілігі әдетте **о-символика** көмегімен беріледі. Бұл математикалық аппарат көмегімен бір шаманың өсу сипатын **(өсу ретін)** басқа шаманың өсуіне байланысты көрсетуге болады.

Түсіндірме. T=O(n) болсын. Сонда кіріс деректерін екі еселеу алгоритмді орындау уақытын екі еселейді. Егер де $T=O(2^n)$ болса, онда кіріс мәліметтеріне бір битті қосу алгоритмді орындау уақытын екі есе көбейтеді.

Қатаң анықтама береміз. Егер $g(n) <= C|f(n)|$, мұнда $n>=N_0$, шартын қанағаттандыратын C және N_0 тұрақтылары табылатын болса, онда теріс емес **g(n) функциясының өсу дәрежесі O(f(n)) болады дейміз.**

Егер алгоритм n өлшемді кіріс деректерін $\tau=cn^2$, c-const, уақыт ішінде өңдесе, онда бұл алгоритмнің уақыттық күрделілігі $O(n^2)$ ("n^2 реттік" деп оқылады) болады.

Алгоритм **тұрақты** деп аталады, егер оның күрделілігі n-нен тәуелсіз болса: O(1). Алгоритмнің уақыттық күрделілігі O(n) болса, онда ол **сызықтық** деп аталады. Егер $T=O(n^2)$ болса, онда алгоритм **квадраттық,** егер $T=O(n^3)$ – **кубтық** деп аталады. Бұлардың барлығы полиномиалдық алгоритмдер. Яғни, полиномиалдық алгоритм немесе полиномиалды уақыттық күрделілік алгоритмі деп уақыт күрделілігі $\tau=O(P(n))$ тең, мұндағы P(n) – әлдебір полином, ал n – есептің (кіріс) көлемі, алгоритмді айтады. Уақыттық күрделілігі $\tau=O(c^{P(n)})$, мұнда c – const, P (n) – полином, болатын алгоритмдер **экспоненциалдық** деп аталады

Ақпарат теориясына сәйкес, бір реттік блокноттардан басқа, барлық криптографиялық алгоритмдерді бұзуға болады. Алгоритмдердің күрделілік теориясы "мұны қандай уақыт ішінде жасауға болады?» сұрағына жауап береді.

Бақылау сұрақтары мен тапсырмалар

1) Блоктық симметриялық шифрлау принциптері. Жалпы сызба
2) Файстель желісі
3) Сұрыптау алгоритмінде кіріс деректері ретінде не болады? Іздеу алгоритмінде кіріс деректері ретінде не болады? Жұп сандарды табу алгоритмінде? Бұл жағдайда кіріс мәліметтерінің өлшемі деп не аталады?
4) Жоғарыдағы алгоритмдерде орындалу уақыты неден тәуелді?
5) N-элементтік жиындарды тікелей таңдау алгоритмінің күрделілігі қандай?
6) DES-ті тікелей бұзу күрделілігі қандай?
7) n кіріс деректерін өңдеу үшін алгоритмге $100n^3+5000n$ операцияларды орындау қажет болсын. Оның уақыттық күрделілігі $O(n^3)$ екенін дәлелдеу.
8) Келесі функцияларды өсу дәрежесі бойынша орналастыру: a) n, b) $n^{1/2}$, c) logn, d) loglogn, e) $\log^2 n$, f) n/logn, g) $(1/3)^n$, h) $(3/2)^n$, i) 9999999.
9) n-нің келесі функцияларын қарастырайық: $f_1(n)=n^2$; $f_2(n)=n^2+78n$; $f_3(n)=n$, егер n тақ болса, және $f_3(n)=n^3$, егер n жұп болса; $f_4(n)=n$, егер $n<25$, және $f_4(n)=n^3$, егер $n>=25$ болса;
Әр функциялар жұбы үшін $f_i(n)$-нің өсу дәрежесі қай жағдайда $O(f_i(n))$ болатынын көрсетіңіз.

Әдебиеттер: [1, 4] – негізгі, [4] – қосымша.

№ 3 дәріс. **Асимметриялық шифрлеу. Криптоберіктік мәселелері. Криптографияның математикалық негіздері**

Мақсаты: Асимметриялық шифрлеу принциптерімен танысу, қажетті математикалық түсініктерге кіріспе. Криптоберіктік мәселелерін үйрену

Дәріс жоспары:

- Асимметриялық шифрлеу. Жалпы идея, симметриялық шифрлеуден айырмашылығы
- Функциялар. Біржақты функциялар
- Тарих (ранецтік криптожүйе. Сипаттама, кілттер генерациясы, талдау)
- Шифрлеудің математикалық негіздері. Топтар, сақиналар, ақырлы өрістер. Сандар теориясының элементтері
- RSA. Кілттер генерациясы, шифрлеу, дешифрлеу, мысалдар
- Криптоберіктік және әлсіздік

Төмендегі кестеде симметриялық алгоритмдердің сипаттамасы, жалпы белгілері, мысалдары берілген.

Асимметриялық криптография (Диффи-Хеллман, 1977)
Қарастырылатын мәселелер: құпиялылықты қамтамасыз ету, түпнұсқалығын, тұтастығын, авторлықты жоққа шығармауды тексеру
Ақпаратты қалай жасыру керек: бір жақты функциялар, қиын есептелетін математикалық есептер: факторизация, дискретті логарифмдер, эллиптикалық қисықтар
Қазіргі компьютерлік. Мақсатына байланысты ашық немесе жабық кілтпен шифрлау: ақпаратты жабу немесе ЭЦҚ пайдалану
Мысалдар: RSA, DSA, ElGamal, Полиг-Хеллман, Рабин схемасы, Вильямс схемасы, МакЭлис схемасы, LUC, ESIGN

Евклид теоремасы (жай сандар туралы) №1. Жай сандар шексіз көп.

Евклид теоремасы (жай сандар туралы) №2. $\forall k \in Z_+$ (1, 2, 3, …) сандар қатарынан үзіліссіз бірінен соң бірі k рет кездесетін құрама сандар табылады.

Теорема (Жай сандардың негізгі қасиеті). Егер $a_1,\ldots,a_k \in Z$, $p \backslash (a_1 \cdot \ldots \cdot a_k) \Rightarrow \exists i \in \{1,\ldots,k\}: p \backslash a_i$.

Теорема (Жай сандардың көбейтіндісіне жіктеудің бірден-бірлігі туралы). $\forall a \in Z$, a>1 үшін бірден-бір $a=p_1 \cdot p_2 \cdot \ldots \cdot p_n$ жіктеуі болады, бұл жерде $\forall i \in \{1,\ldots,n\}$, p_i – жай сан.

φ(a) **Эйлер функциясы** 0, 1, …, a–1 қатарының a ($a \in Z_+$) санымен өзара жай мүшелерінің санын береді.

Егер 2 бүтін a және b сандарын m-ге бөлу бірдей қалдық беретін болса, онда олар **m модулі бойынша теңқалдықты** немесе **салыстырымды** деп аталады және $a \equiv b \pmod m$ деп жазылады.

Егер $a \cdot b \equiv 1 \pmod m$ болса, b элементін a-ға **m модулі бойынша кері** деп атайды және $b \equiv a^{-1} \pmod m$ деп жазады.

Керілеу теоремасы. $\exists\, a^{-1} \pmod m \Leftrightarrow (a, m)=1$.

Берілген • бинарлық операциясы бар G жиыны **топ** деп аталады, егер:

а) Операция • ассоциативті, яғни $\forall$ a,b,c∈G үшін (a•b)•c=a•(b•c) теңдігі орындалады;

б) $\exists e \in G: \ \forall a \in G \Rightarrow$ a•e=e•a=a (егер топтық операция қосынды деп аталса, онда e нөлдік элемент деп аталады, егер операция – көбейту болса, онда e бірлік элемент деп аталады);

в) $\forall x \in G \ \ \exists x' \in G: \ x \cdot x' = x' \cdot x = e$ (егер топтық операция қосынды деп аталатын болса, онда х′ элементі х–ке қарсы элемент деп аталады, егер операция көбейту болса, онда кері элемент).

Егер топ операциясы <G,•> коммутативті болса (яғни $\forall a,b \in G \ \ a \cdot b = b \cdot a$), онда топ **коммутативті** немесе **Абельдік** деп аталады.

RSA криптожүйесінде әртүрлі *p* және *q* үлкен жай сандары таңдап алынып, $n=pq$, $\varphi(n)=(p-1)(q-1)$ есептеледі, $2<e<n$, $(e, \varphi(n))=1$ шарттарын қанағаттандыратын e саны таңдап алынып, $d=e-1(mod\varphi(n))$ есептеледі. Ашық кілт ретінде (*n, e*) жұбы, жабық, құпия кілт ретінде $(p, q, \varphi(n), d)$ төрттігі алынады.

Бақылау сұрақтары мен тапсырмалары

1) Асимметриялық шифрлау принциптері. Жалпы идея. Мысалдар
2) Қарапайым сандар туралы негізгі теоремалардың дәлелдемелерін келтіру
3) Модуль бойынша салыстыру анықтамасын беру және салыстыру қасиеттерін келтіру
4) Модуль бойынша кері элемент және криптографиядағы осы ұғымның рөлі
5) Топты, өрісті анықтау. Мысалдар келтіріңіз
6) Сандарды факторизациялау мәселесі
7) RSA схемасы
8) Дискретті логарифмдеу есебі
9) ElGamal схемасы
10) Эллипстік қисықтар

Әдебиеттер: [1, 4] – нег., [4] – қосымша.

№4 дәріс. **Асимметриялық шифрлеудің алгоритмдері. Криптографиялық хэш-функциялар. Цифрлық қолтаңбалар. Криптобериктік мәселелері**

Мақсаты: ақпаратты қорғауға арналған криптографиялық хэш-функциялар мен асимметриялық шифрлеу алгоритмдерін қолдану мәселелерін үйрену

Дәріс жоспары:

- асимметриялық шифрлеу алгоритмдері. Асимметриялық –кілттік криптографиялық жүйелер: Рабиннің (Rabin), Эль-Гамалдің (ElGamal), эллипстік қисық тәсілі негізіндегі криптожүйе (ECC – Elliptic Curve Cryptosystem), олардың қауіпсіздігі
- Хаттың бүтіндігі мен дұрыстығы
-Криптографиялық хэш-функция. Меркл-Дамгард (Merkle-Damgard) сызбанұсқасы
- Хэш-функция сығу (SHA) функциясы және (Whirlpool) блоктық шифры тұрғысынан
- SHA жиынтығының хэш-функциялары, RIPMD және HAVAL алгоритмдері
- Рабин, Матис-Мейер-Осеас (Metyas-Mayer-Oseas), Миагучи-Пренель, Whirlpool сызбанұсқалары
- Электронды қолтаңба. Цифрлық қолтаңбалардың (RSA, Эль-Гамаль (ElGamal), Шнорр (Schnorr), DSS, эллипстік қисық) сызбанұсқалары. Цифрлық қолтаңбалар қосымшалары

ElGamal шифры – теориялық-сандық мәселелерге негізделген асимметриялық шифр. Жүйенің параметрлері: p – жай сан, α – Up тобын туындататын элемент; ашық текстi қалпына келтіруге арналған жабық кілт: a – бүтін сан, $1 \le a < p-1$; шифрлауға арналған ашық кілт: $\beta=\alpha^a \bmod p$.

Ашық текст $x \in Up$ берілсін дейік. Шифрлеу үшін кездейсоқ $k \in Z_{p-1}$ санын алып, $y_1=\alpha^k \bmod p$, $y_2=x\beta^k \bmod p$ шамалары есептеледі. Содан кейін (y_1,y_2) жұбы құпия кілт иесіне жіберіледі, ал k жойылады. Ашық текстi қалпына келтіру үшін $x=y_2(y_1^a)^{-1} \bmod p$ шамасын есептеп шығару керек. Шынында да, нәтижесінде ашық мәтінді аламыз:

$y_2(y_1^a)^{-1}modp=x\beta^k(\alpha^{ka})^{-1}modp=x\alpha^{ak}(\alpha^{ka})^{-1}modp=x\alpha^0\ modp=x.$

Хештеу немесе **хэштеу** (ағылш. hashing) — ұзындығы кез келген кіріс деректер массивін белгілі бір алгоритммен есептелетін ұзындығы алдын-ала белгілі (шығыс) биттер жолына түрлендіру. Алгоритмді жүзеге асыратын және түрлендіруді орындайтын функция "**хеш-функция**" немесе "**жинақтау функциясы**" деп аталады. Бастапқы деректер кіріс массиві, "кілт" немесе "хабар" деп аталады. Түрлендіру нәтижесі (шығыс мәліметтері) "**хеш**", "**хеш-код**", "**хеш-сома**", "**хабар сығындысы**" деп аталады.

Бастапқы мәтін бір ғана символға өзгергеннің өзінде, хеш функцияның нәтижесі толығымен өзгереді. Хеш-функциялардың бұл қасиеті оларды сандық қолтаңбалар үшін қолдануға мүмкіндік береді.

Криптографиялық хеш-функциялар — оларды криптографияда қолдануға жарамды ететін белгілі бір қасиеттері бар хеш-функциялар класы.

Жалпы жағдайда хеш-функцияны құру негізінде итеративті тізбекті схема жатады. Алгоритмнің ядросы қысу функциясы болып табылады — k кіріс биттерін n шығыс биттеріне түрлендіру, мұндағы n — хэш-функцияның разрядтылығы, ал k — n-нен үлкен кез келген сан. Бұл ретте қысу функциясы криптотөзімділіктің барлық шарттарын қанағаттандыруы тиіс. Кіріс ағыны (k − n) биттен тұратын блоктарға бөлінеді. Алгоритм бастапқы мәні ретінде жалпыға белгілі әлдебір сан алынатын n-биттен тұратын уақытша айнымалыны пайдаланады. Әрбір келесі деректер блогы қысу функциясының алдыңғы итерациядағы шығыс мәнімен біріктіріледі. Хеш-функцияның мәні ретінде соңғы итерацияның шығыс n биті алынады. Хеш-функцияның шығыс мәнінің әрбір биті барлық кіріс деректер ағынынан және бастапқы мәннен тәуелді. Осылайша, тасқын әсері жүзеге асады.

Бақылау сұрақтары мен тапсырмалар

1) Рабин (Rabin), Эль-Гамаль (Elgamal) криптографиялық жүйелерінің схемалары, олардың қауіпсіздігі
2) Хабарламалардың тұтастығы мен түпнұсқалығын қамтамасыз ету мәселелері
3) Криптографиялық хэш-функцияларды анықтау және мысалдар
4) Электрондық қолтаңба. Цифрлық қолтаңба схемалары (RSA, Эль-Гамаль (ElGamal), Шнорр (Schnorr), DSS, эллипстік қисық). Сандық қолтаңбалардың қосымшалары

Әдебиеттер: [1, 4-7] – нег., [1-4] - қос.

№ 5 дәріс. **Криптоталдауға арналған программалық-аппараттық криптографиялық құралдар мен аспаптар. Криптографиялық алгоритмдер мен криптографиялық хаттамалардың әлсіздігі**

Мақсаты: Криптоталдау есептерін шешуге және криптографиялық қосымшаларды құрастыруға арналған заманауи аспаптармен танысу. Криптографиялық шабуылдарды тәжірибелік жүзеге асыру негізінен қарағанда криптографияның заманауи алгоритмдерінің криптоберіктік және әлсіздік мәселелерін оқу

Дәріс жоспары:

- Программалық және программа-аппараттық криптографиялық құралдардың классификациясы мен жобалары.
- Криптоталдаудың программалық құралдарының классификациясы және оларға шолу (ғылыми есептеулерге арналған қолданбалы пакеттер және шифрлеу алгоритмдері, криптографиялық хэш-функцияларды криптоталдауға арналған басқа да программалық қамтамалар)
- Криптоталдаудың программалық құралдарының тиімділігін салыстыру

- Криптографиялық алгоритмдер мен криптографиялық хаттамалардың әлсіздігі

Криптоанализдің қазіргі практикалық міндеттерін орындау үшін қуаты жеткілікті есептеуіш компьютерлер қажет. Көптеген жағдайларда әңгіме таратылған жүйелер мен суперкомпьютерлер туралы. Криптоанализге арналған оқу есептерінде әдетте криптографиялық алгоритмдердің қатты оңайлатылған модельдері қарастырылады. Дегенмен, бұл жағдайда да өнімділігі жоғары топқа жататын процессоры бар ДК қажет.

Бұл жерде қарастырылатын мәселелер ерекшелігімен байланысты бағдарламалардың орындалу жылдамдығына қойылатын талап туралы айта кету керек. Осыған байланысты бағдарламалау тілі ретінде ассемблерді (кейбір қосымша мәселелерді іске асыруда), ал көпшілік жағдайда C/C++ тілдерін қолданған жөн. Сондай-ақ, мәселелердің ерекшелігі үлкен сандармен жұмыс істеуді қамтамасыз етуді талап етеді. Бұл жерде көп жағдайда Python тілін қолдануға болатынын айтамыз, өйткені оның интерпретаторы үлкен сандармен жұмыс істеуге мүмкіндік береді. Сондай-ақ үлкен сандармен жұмыс істеуге арналған кітапханалар қажет, жоғарыда айтылғандарға байланысты, әсіресе C/C++тілдері үшін. Бұл салада танымал GMP кітапханасына тоқтауға болады. Жоғарыда айтылғандар мынадай тұжырымға әкеледі: бағдарламалық іске асыру командалық жолдың интерфейсін ұстануы тиіс. Мұнда терминал/командалық жолда жұмыс істеу дағдысы болу қажеттілігі туралы мәселе туындайды. Бағдарламаларды іске қосуды және орындауды жеңілдететін басқарушы скрипттер жасай білу қажет. Бастапқы кодтардан бағдарламалық қамтамасыз етуді (кітапханаларды) құрастыру дағдылары да болуы қажет.

Суперкомпьютерлердің операциялық жүйелері басым көпшілік жағдайда Linux болып табылатындықтан, Linux утилиталарын білу қажет. Суперкомпьютерлермен жұмыс қашықтан SSH-хаттама арқылы жүзеге асырылады, ол үшін интерфейсті қамтамасыз ететін арнайы бағдарламаларды білу қажет.
Windows үшін MSYS пакеті бір жағынан bash қабыршағын қолдану мүмкіндігін қамтамасыз етеді, екінші жағынан, оның құрамындағы утилиталар кейбір кітапханаларды жинау үшін қажет.

Сондай-ақ криптоанализ міндеттерімен тікелей байланысы жоқ, бірақ оларды жеңілдететін басқа да пайдалы бағдарламалық құралдар туралы айта кету керек. Бұл ыңғайлы көпфункционалды файлдық менеджерлер, екілік файл редакторлары, make типті утилиталар, түрлі архиваторлар және т. б.

Криптографиялық кітапханалар криптографиялық примитивтерді жүзеге асыру үшін қажет, олардың көмегімен шифрматериалдарын қажетті мөлшерде және белгілі бір параметрлермен генерациялауға болады. Шифрматериалдар криптоанализ және криптографиялық шабуылдарды зерттеу үшін қажет.

Криптоанализ әдістері іске асырылған БҚ арасында CrypTool құралдарын атап өтуге болады. CrypTool-да шифрлеу/шифрлеу және криптоанализдеу әдістері, классика шифрлары және қазіргі заманғы компьютерлік.

Бақылау сұрақтары мен тапсырмалары

1) Бағдарламалық және бағдарламалық-аппараттық криптографиялық құралдарға шолу және жіктеу
2) Криптоанализ бағдарламалық құралдарына шолу және жіктеуді орындау (ғылыми есептеулерге арналған қолданбалы пакеттер және шифрлау алгоритмдерінің криптоанализіне арналған басқа бағдарламалық қамтамасыз ету, криптографиялық хэш-функциялар)
3) Ұсынылған құралды орнату

Әдебиеттер: [оқытушы материалдары, БҚ ресми сайттары].

№ 6 дәріс. **Криптоталдау есептерін шешуге арналған аспаптарды құру мен қосымшаларды жасау мәселелері**

Мақсаты: Криптоталдау есептерін шешуге арналған және тәжірибелік сұрақтармен сәйкес келетін аспаптарды құру мен қосымшаларды жасауды қарастыру. Криптоталдауға арналған программалық құралдарды жасау мүмкіндіктерін зерттеу

Дәріс жоспары:

- Ғылыми есептеулерге арналған қолданбалы пакеттердің көмегімен программалау
- Криптографиялық кітапханалар
- C++ тілі үшін үлкен сандармен жұмыс жасауға арналған кітапханалар және оларды криптоталдау есептерінде қолдану
- Параллельді есептеуге арналған C++11 (C++14) стандарттарының құралдары, таратылған есептеулерге арналған MPI интерфейсі. Криптошабуылдарда қолдану (таратылған деректермен берілген есептер –Brute force әдісін, слайдтық шабуылдар, және т.б. жүзеге асыру)
- Криптоталдау кітапханалары мен аспаптары және оларды қолдану мысалдары (CrypTool және басқа да плагиндерін жасау)
- Криптоталдауға арналған ашық қосымшалардың кодтарын талдау (кітапханалар, CrypTool, басқалар)
- Криптографиялық талдауға арналған қосымшаларды әзірлеудің тәжірибелік мәселелері және көмекші аспаптық құралдар (терминал, файл-менеджерлер, скрипттік тілдер, командалық қабықтардың сценарийлері, (bash-скрипт, Windows-тың командалық файлдары), бинарлық (оналтылық) файлдардың редакторлары, компиляторлар)

Mathematica — ғылыми, инженерлік, математикалық және компьютерлік салаларда кеңінен қолданылатын компьютерлік алгебра жүйесі (әдетте Математика, Математика бағдарламалық пакеті деп аталады).

Sage — алгебра, комбинаторика, есептеу математикасы және матанализді қоса алғанда, математиканың көп салаларын қамтитын компьютерлік алгебра жүйесі.

Maple — бағдарламалық пакет, компьютерлік алгебра жүйесі (дәлірек айтқанда, компьютерлік математика жүйесі). Waterloo Maple Inc. компаниясының өнімі болып табылады. 1984 жылдан бастап күрделі математикалық есептеулерге, деректерді визуализациялауға және моделдеуге бағытталған бағдарламалық өнімдерді шығарады.

GNU Compiler Collection (әдетте GCC деп қысқартылады) — әр түрлі бағдарламалау тілдерінің компиляторлары жиынтығы. GCC — ақысыз таратылатын өнім. Ол коммерциялық емес UNIX-типтес операциялық жүйелер үшін стандартты компилятор ретінде пайдаланылады.

MinGW — Windows операциялық жүйелері үшін программаларды жазуға арналған әзірлеу құралдарының жиынтығы. Оған Windows API үшін еркін таратылатын импорт кітапханалары мен тақырып файлдарының жиынтығымен бірге Windows-қа көшірілген GNU Compiler Collection (GCC) компиляторларының порты, әр түрлі көмекші утилиталар кіреді.

Crypto++ — криптографиялық алгоритмдер мен схемалар үшін Вэй Дай жазған C++ кластарының еркін және ашық кітапханасы. Crypto++ академиялық ортада, студенттік жобаларда, ашық бастапқы коды бар жобаларда және коммерциялық емес жобаларда, сондай-ақ бизнесте кеңінен қолданылады.

GMP немесе GNU Multi-Precision Library — қалаулы дәлдікпен жылжымалы үтірлі, бүтін және рационалды сандармен есептеу жұмыстарын жүргізуге арналған C тілінде жазылған кітапхана. Кітапхана криптографиялық мақсатта және компьютерлік есептеулер үшін кеңінен қолданылады. Бұл кітапхана gcc-ті жинау үшін қажет.

Бақылау сұрақтары мен тапсырмалары

1) Mathematica, Maple, Sage пакеттерінің сипаттамасын беру, олардың негізгі мүмкіндіктерін атап көрсету және мысалдар келтіру.
2) GPG және CrypTool пакеттерінің сипаттамасын беру, олардың негізгі мүмкіндіктерін көрсету және мысалдар келтіру.
3) gcc/MinGW компиляторларының, Python интерпретаторының сипаттамасын беріңіз. Оларды криптография және криптоанализдің практикалық есептерінде қолдануды негіздеу.
4) C++ үшін үлкен сандармен жұмыс істеу кітапханаларын сипаттау, мысалдар келтіру.
5) C++ үшін криптографиялық кітапханаларды сипаттау, мысалдар келтіру.
6) Компьютерде қашықтан жұмыс істеу үшін ыңғайлы интерфейсті қамтамасыз ететін программаларды сипаттау (PuTTY, WinSCP).
Әдебиеттер: [оқытушы материалдары].

Дәріс № 7. **Классикалық шифрлерді криптоталдау**
Мақсаты: Классикалық шифрлерді криптоталдау әдістерін және оларды қолдануға арналған программалық қамтамаларды оқу. Аспаптарды құру мәселелері
Дәріс жоспары:
- Классикалық шифрлерді криптоталдау әдістері. Тілдің жиілік талдауы. Қазақ тілінің жиілік талдауы. Криптоталдауда қолдану.
- Классикалық шифрлерді криптоталдауға арналған программалық қамтамалар. Web-қосымшалар
- Классикалық шифрлерді криптоталдауға арналған қосымшаларды құру

Біралфавитті алмастыру жүйесіне қарсы криптоталдаушы шабуыл символдардың жиілігін есептеуден басталады, яғни шифрланған мәтіндегі әрбір әріптердің саны анықталады. Шифрланған мәтіндегі әріптердің жиілігі бастапқы хабар алфавитіндегі әріптердің жиілігімен салыстырылады.

Омофондар жүйесі – шифр мәтініндегі әріптердің пайда болу жиілігінің есебіне негізделген, криптоаналитикалық шабуылдардан қарапайым қорғануды қамтамасыз етеді. Берілген хабарлар әріптері бірнеше алмастыруларды иемденетін болса да, омофондар жүйесі бір алфавитті болып табылады. Алмастырулар саны ашық мәтіндегі әріптердің пайда болу ықтималдығына пропорционал алынады.

Плейфейр шифры – ең танымалы биграмдық шифр. Негізгі шифр берілген хабардың әріптерінің кез келген ретпен орналасқан кестесі болып табылады.

Берілген хабардың әрбір символын шифрлау үшін қарапайым алмастырудың өз шифры қолданылатын болғандықтан, күрделі алмастыру шифрлары көп алфавитті деп аталады. Көп алфавитті қойылым қолданылатын алфавиттерді тізбектеп және цикіл бойынша өзгертеді.

Гамма әдісімен алынған шифрмәтінді шешу айтарлықтай қиынға түседі, себебі кілт мұнда айнымалы болып табылады.

Шифрлау алгоритмдерін компьютерлік іске асыру және орыс, әсіресемен қазақ тіліндегі мәтіндерге арналған криптоталдау әдістері мәселелерінде қолданбаларда және командалық жолда/терминалда символдарды кодтауға байланысты проблеманы атап өткен жөн.

Бақылау сұрақтары мен тапсырмалары
1) Классикалық шифрлардың криптоанализ әдістерін сипаттау.
2) Тілдің жиіліктік талдауы және оның мәтіндік алгоритмдердің криптоанализіндегі рөлі.

3) Зерттеу жүргізу: қазақ тілінің жиіліктік талдауы.
4) Алынған нәтижелерді криптоанализге өз нұсқасына сәйкес қолдану.
5) Классикалық шифрлардың криптоанализіне арналған программалық құралдарға шолу жасау.
Әдебиеттер: [1, 4-7] – осн., [1-4] – қосымша; Әбдіқалықов Қ. Ә. Криптографияның негіздері: оқулық.

Дәріс № 8. **Симметриялық шифрларды криптоталдаудың әдістері I**
Мақсаты: Симметриялық шифрлеу алгоритмдерін криптоталдау әдістері мен криптоберіктік сұрақтарын оқу
Дәріс жоспары:
- Заманауи шифрлердің криптоберіктігін зерттеу. Алгоритмдердің әлсіздігі
- Кілттерді басқару, генерациялау мәселелері
- Ортада кездесу әдісі
- Сызықтық криптоталдау әдісі

Ортада кездесу әдісі. Егер криптоалгоритм кілттерінің жиыны композицияға қатысты тұйық болса, яғни кез келген z_i және z_j кілттері үшін z_i және z_j-мен кез келген мәтінді тізбектеп шифрлеу нәтижесі z_k-пен осы текстің шифрограммасына тең болатындай z_k кілті табылса, яғни $F(z_j, F(z_i, x)) = F(z_k, x)$, онда осы қасиетті қолдануға болады. z_k кілтін табу керек болсын. Онда z_k кілтін табу үшін оған балама z_i, z_j кілттерін табу қажет. Бұл криптоанализ әдісі "туған күндердің парадоксіне" негізделген. Егер туған күндер біркелкі үлестірілсе, онда 24 адамнан тұратын топта 0,5 ықтималдықпен екі адамның туған күндері сәйкес келеді. Егер $ab^{1/2}$ заттар b өлшемді әлдебір жиынтықтан қайтарып оралумен таңдалатын болса, онда олардың екеуінің бірдей болу ықтималдығы $1-\exp(a^2/2)$-ге тең (сипатталған жеке жағдайда b=365 – жылдағы күн саны, $ab^{1/2}=23$, яғни а шамамен 1,256-ға тең).

Криптоанализде бұл парадокс былай қолданылады. Айталық, С – бос емес жиын, ал А мен В – С жиынының ішкі жиындары. Егер олардың өлшемдері келесі ab>=c, мұнда а – А жиынының мөлшері, b – В жиынының мөлшері, с – С жиынының мөлшері, шартын қанағаттандырса, онда А мен В жиындары ең болмағанда бір рет қиылысады деп үлкен сеніммен айтуға болады.

Әдістің күрделілігі $O(\log a)$. Алгоритм ықтималдық болып табылады. Алайда, осы алгоритмінің американдық математик Д. Шенкс ұсынған "giant step-baby step" атты детерминденген аналогы бар.

Сызықтық криптоанализ. Бұл шифрлеу теңдеулері үшін сызықтық статаналогтарды іздеуді, қолда бар ашық және шифрленген мәтіндерді статистикалық талдауды үйлестіретін құрамдастырылған әдіс, сондай-ақ келісу және таңдау әдістерін пайдаланатын. Бұл әдіс ашық мәтін, тиісті шифртекст және кілт векторларының жеке координаттары арасындағы статистикалық сызықтық қатынастарды зерттейді және осы қатынастарды кілт векторының жеке координаттарын статистикалық әдістермен анықтау үшін қолданады.

Бүгінгі күні сызықтық криптоанализ әдісі блоктық шифрлаудың итерациялық жүйелерінің бірқатарын, оның ішінде DES жүйесін, ашу бойынша анағұрлым күшті нәтижелер алуға мүмкіндік берді. Әдіс FEAL блоктық шифрлау жүйесін талдау кезінде айқын емес түрде қолданылды.

Бекітілген $k \in Z^{2k}$ кілт үшін ашық текст $p \in Z^{2n}$ векторын шифртекст $c \in Z^{2n}$ векторына бейнелейтін $F: Z^{2n} \times Z^{k2} \rightarrow Z^{2n}$ блоктық шифры берілсін. Ашық текст кездейсоқ және бірдей ықтималдықпен таңдалады, ал кілттер әрбір раундта бір-бірінен тәуелсіз. Шабуылдың күрделілігі қажетті белгілі ашық мәтіндердің санымен байланысты, өйткені кез келген жұп

үшін (ашық мәтін, шифртекст) алгоритмді жүзеге асыру үшін есептеу мөлшері көп қажет емес. Тек шифртекст бар болса, бұл шабуылды жасауға болады.

Бақылау сұрақтары мен тапсырмалары
1) Криптографиялық алгоритмдердің осалдығының мәні
2) Кілттердің әлсіздігі түсінігі. Кілттерді басқарудағы, генерациялаудағы осалдықтар
3) Ортада кездесу әдісін сипаттау
4) Сызықтық криптоанализ әдісін сипаттау.
Әдебиеттер: [1-4] - негг. [1-4] - қос.; С. М. Авдошин, А. А. Савельева «Криптоанализ: современное состояние и перспективы развития»

Дәріс № 9. **Симметриялық шифрларды криптоталдаудың әдістері II**
Мақсаты: Симметриялық шифрлеудің алгоритмдерін криптоталдау әдістері мен криптобериктік сұрақтарын оқу
Дәріс жоспары:
- Дифференциалды криптоталдау әдісі
- Алгебралық талдау
- «Квадрат» типті шабуыл
- Өз-өзіне ұқсауға негізделген шабуылдар. Слайдтық шабуыл
- Туған күндер парадоксы және оның криптоталдау есептеріндегі орны

Айырымдық талдау әдісі зерттеудің ықтимал-статистикалық әдістерін қолдана отырып, жалпы сызықтық құрылым идеясын қорытуды қамтиды. Бұл әдіс таңдалған ашық мәтін бойынша шабуылдарға жатады. Белгілі ашық мәтінге айырымдық талдауды қолдану әрекеттері көп жағдайда талап етілетін материалдың күрт өсуіне алып келді. Әдісті 1990 жылы Израиль математиктері Э. Бихам мен А. Шамир әзірледі. Дифференциалдық талдау әдісіне жақын идеяны 1990 жылы С. Мерфи Э. Бихам мен А. Шамирдің жұмысына дейін жариялады. Әдіс кейбір тіркелген айырмашылығы бар ашық мәтіндердің жұптарынан алынған екі шифртекстің айырмаларының мәндерінің үлестірілуінің тең ықтималды еместігін пайдалануға негізделген.

Криптоанализдің алгебралық әдістері келесі кезеңдерден тұрады:
- S-блоктардағы түрлендіруді сипаттайтын теңдеулердің сызықты емес жүйесін құру;
- сызықты емес жүйені шешу.

Криптоанализде буль теңдеулерінің сызықты емес жүйелерін шешудің әртүрлі тәсілдері әзірленді. Криптоанализ тәжірибесі көрсеткендей, ең тиімді болып бастапқы жүйенің линеаризациясын пайдаланатын әдістер табылады. XL алгебралық криптоанализ әдісін (eXtended Linearization) N. Courtois, A. Klimov, J. Patarin және A. Shamir ұжымы ұсынған.

Слайдтық шабуыл – таңдалған ашық мәтін негізіндегі криптографиялық шабуыл, ол көп раундтық блокты шифрлардың криптоанализін жүргізуге мүмкіндік береді. Шабуылдың мұндай түрін алғаш рет 1999 жылы Алекс Бирюков пен Дэвид Вагнер ұсынды. Слайдтық шабуылдың негізін екі түсінік құрайды:

1. Шифрлау раундтарының ұқсастығы – әрбір раунд үшін F () функциясы бірдей;

2. Кілтті табу мүмкіндігі – кез-келген раундтың кірісінде және шығысында тексті біле отырып, берілген P және F(P) арқылы K-ны табуға болады.

Идея шифрлеудің екі процесін бір-бірінен бір раундқа қалыс қалатындай етіп өзара салыстыру болып табылады. Слайдты жұбын тапқаннан кейін кілттің кейбір биттердің табуға болады. Қалған биттерді табу үшін басқа слайд жұбын табу және оның көмегімен талдау жүргізу қажет. Бірнеше слайдтық жұптарды табу нәтижесінде кілттің барлық биттерін табу мүмкіндігі пайда болады.

Бақылау сұрақтары мен тапсырмалары
1) Дифференциалдық криптоанализде қолданылатын математикалық ұғымдарды сипаттау
2) Сызықтық криптоанализ әдісін сипаттау
3) Алгебралық криптоанализдің мәнін сипаттау
4) Слайдтық шабуылды сипаттау.
Әдебиеттер: [1-4] - нег. [1-4] - қос.; С. М. Авдошин, А. А. Савельева «Криптоанализ: современное состояние и перспективы развития» , Л. К. Бабенко, Е. А. Маро «Алгебраический криптоанализ упрощенного алгоритма шифрования Rijndael»

Дәріс № 10-11. **Заманауи симметриялық шифрларды криптоталдау**
Мақсаты: Симметриялық шифрлеудің алгоритмдерін криптоталдауға арналған программалық қамтаманы қолдану
Дәріс жоспары:
- Криптоталдаудың симметриялық алгоритмдерін криптоталдау кезінде қолданбалы пакеттердің қолданылуы
- Программалық құралдардың көмегімен симметриялық шифрлеудің алгоритмдерін криптоталдау
- Қолданылған программалық құралдар жұмысын салыстыру

Maple, Mathematica, Sage сияқты пакеттерде барлық криптографиялық алгоритмдердің математикалық аппараты іске асырылған. Пакеттер криптография және криптографиялық шабуылдар алгоритмдерінің толық бағдарламалық кодтарымен файлдарды жасауға мүмкіндік береді. Кодты басқа тілдерден интеграциялау мүмкіндігін, сондай-ақ басқа тілдердегі кодты генерациялау мүмкіндігін қолдайды. Mathematica және Sage пакеттерінің web-интерфейсі бар.

S-DES, бір раундтық AES алгоритмдері үшін тікелей аралық, сызықтық және дифференциалды талдау сияқты криптографиялық шабуылдардың C тілінде жүзеге асырылуы бар. Тура іріктеу алгоритмі бөлінетін мәліметтері бар алгоритм болғандықтан, параллельдеуге жол береді. Мұнда қолайлы құралдар MPI интерфейсі және стандартты C++ (Thread класы) құралдары болады. Есептеу кластерлерін пайдалану мүмкіндігі кейбір жағдайларда толық криптоанализге қол жеткізуге мүмкіндік береді. Ал, симметриялы алгоритмдерді шифрлаудың кейбір режимдерін іске асыру үшін параллельді бағдарламалау әдістерін қолдану мәселесі біршама қиын.

Ақырында, қазіргі заманғы криптожүйелердің тиісті түрде іске асырылған барлық практикалық ұсынымдарды сақтаған жағдайда алгоритмдер мен кілттердің жұмысы туралы кейбір ақпаратты алу туралы ғана айтуға болады. Және мұндай ақпарат криптожүйенің қорғалуына айтарлықтай әсер етуі екіталай. Дегенмен, мұндай нәтиже (кейбір ақпарат) криптоанализдің нөлдік емес нәтижесі болып саналады.

Бақылау сұрақтары мен тапсырмалары
1) Криптографияда қолданылатын математикалық пакеттердегі функцияларды жүзеге асырумен танысу. Қарастырылған пакеттерде криптографиялық алгоритмдерді іске асыру мәніне салыстырмалы талдау жүргізу.
2) Криптоанализдегі математикалық пакеттердің мүмкіндіктерін сипаттау. Бар іске асыруға шолу жасау.
3) Әртүрлі бағдарламалау тілдерінде криптоанализ әдістерін жүзеге асыру мүмкіндіктерін сипаттау. Салыстырмалы талдау жасау.

Әдебиеттер: [1] – осн., ғылыми-практикалық әзірлемелердің қол жетімді жарияланымдары, интернет материалдары

№ 12 дәріс. **Асимметриялық шифрлеу алгоритмдерін криптоталдаудың әдістері. Хэш-функцияларға шабуылдар және цифрлық қолтаңбалар**

Мақсаты: Цифрлық қолтаңбалар, криптографиялық хэш-функциялар, асимметриялық шифрлеу алгоритмдерінің криптоберіктік мәселелерін қарастыру

Дәріс жоспары:

- Заманауи шифрлердің криптоберіктігін зерттеу
- Ашық кілтті криптографиялық жүйелерге жасалатын шабуылдар. Ортада кездесу әдісі
- Бөліктеу
- Дискретті логарифмдер
- Эллипстік қисық
- Торлы криптоталдау әдісі
- Хаттама, режим, инициализация әдістері
- Шет каналдар арқылы шабуылдау
- RSA шабуылдары, мысалдар
- «Асимметриялық шифрлеудің тиімді толықтырылуы» процесі - OAEP (Optimal Assimetric Encryption Padding)
- Хэш-функциялар шабуылдары
- Цифрлық қолтаңбалар шабуылы

Үлкен бүтін N санын **көбейткіштерге жіктеу (факторизациялау) есебі** субэкспоненциалды алгоритмдер класына жатады, олардың күрделілігі $L_N[a,b]=\exp((b+o(1))\log N)^a(\log\log N)^{1-a}$ шамасын құрайды. GNFS (General Number Field Sieve – жалпы түрдегі сандар өрісінің торы) алгоритмінің күрделілігі $L_N[1/3, (64/9)^{1/3}]$ шамасын құрайды. SNFS (Special Number Field Sieve – арнайы $N=a^b+c$ түріндегі сандар өрісінің торы) алгоритмінің күрделілігі $L_N[1/3, (32/9)^{1/3}]$ шамасын құрайды. O(logN) кубиттік кванттық компьютерді пайдалана отырып шешу күрделілігі O(logN) шамасын құрайды. 1024 битке дейінгі екілік ұзындықтағы сандарды факторизациялау үшін ECC (Elliptic Curve Method) алгоритмінің ең қолайлылығы белгілі, үлкен мөлшердегі сандарға эллипстік қисықтарды пайдаланатын GNFS алгоритмі қолданылады.

Бүтін сандарды көбейткіштерге жіктеудің тиімді тәсілдерін іздеумен адамдар бұрыннан айналысады. n санын көбейткіштерге жіктеудің ең айқын әдісі – саны $n^{1/2}$–ден аспайтын қарапайым бөлгіштерді қарап шығу. Сондай−ақ, басқа аралықты әдіс бар (Ферма әдісі), ол n санының квадраттар айырмасы түрінде жазуға негізделген: $n=a^2-b^2=(a+b)(a-b)$. Күрделілігіне қарай, қарапайым аралық әдіс, сондай-ақ Ферма әдісі $O(n^{1/2})$ шамасымен бағаланады, бірақ соңғы әдіс, егер n санының бөлгіштері бір-біріне жақын болса, тиімді болуы мүмкін. Үлкен n сандары үшін мұндай алгоритмдердің жұмыс уақыты тиімсіз болады. Мұндай сандарды факторизациялауға кіріспес бұрын, олардың шын мәнінде құрамдас екеніне көз жеткізу керек. Ол үшін, мысалы, Миллер-Рабин алгоритмі сияқты қарапайымдылықты тексерудің ықтималдық тесттерінің бірін қолданған жөн.

Сандарды көбейткіштерге жіктеудің тиімдірек әдістері де бар – мысалы күрделілік бағасы субэкспоненциалды әдістер. Мәселен, эллипстік қисықтардың көмегімен бүтін сандарды факторизациялауға арналған Ленстраның ықтималдық алгоритмінің уақыт бойынша күрделілігінің орташа бағасы $\exp(((2+o(1))\log p \log\log p)^{1/2})\log^2 n$, мұндағы p – n санының ең кішкентай қарапайым бөлгіші. p-ны n-ге ауыстырғанда күрделіліктің субэкспоненциалды $L_N[1/2;2]$ бағасын аламыз. Бұл әдісті шағын қарапайым бөлгіштерді

бөліп алу үшін тиімді пайдалануға болады. Әдістің артықшылығы – жады көлемін аз пайдаланады. Факторизацияның тағы бір субэкспоненциалды алгоритмі – Диксон әдісі.

Дискретті логарифмдеу есебі – бір-бірінен тек топтарды құрайтын алгебралық құрылымдармен ғана ерекшеленетін есептердің тұтас класы. Шектелген циклдық n-реттік <G> тобы, құрушы элемент P және топтың кез-келген Q элементі берілсін. Дискретті логарифмді табу есебі Q=xP (сан n модулі бойынша келтірілген) теңдеуін қанағаттандыратын x бүтін санын іздеуден тұрады. Дискретті логарифмдеу есебі факторизация есебінен гөрі күрделірек болып саналады. Егер оны шешудің полиномиалдық алгоритмі табылса, көбейткіштерге жіктеу (керісі дәлелденбеген) мүмкін болады.

Есептеу күрделілігі теориясының соңғы жетістіктері ақырлы өрістерде логарифмдеудің жалпы проблемасы жеткілікті берік іргетас болып саналмайтынын көрсетті. Қазіргі таңда ең тиімді дискретті логарифмдеу алгоритмдері экспоненциалды емес, субэкспоненциалды уақыттық күрделілікке ие. Бұл жіктеу базасын қолданатын "index-calculus" алгоритмдері. Бірінші мұндай алгоритмді Адлеманмен ұсынды.

Криптоанализдің көптеген есептері, мысалы, есептелетін рет тобында логарифмдеу немесе хэш-функция коллизияларын іздеу, Поллард алгоритмімен шешілетін кездейсоқ бейнелеу графындағы кездесу туралы есепке келтіріледі.

Бақылау сұрақтары мен тапсырмалары

1) Асимметриялық алгоритмдер идеясын сипаттау
2) RSA криптоталдау әдістерін сипаттау
3) ElGamal криптоталдау әдістерін сипаттау
4) Асимметриялық алгоритмдердің криптоталдау күрделілігінің салыстырмалы талдауын орындау

Әдебиеттер: [1-4] - негі. [1-4] - қос.;
http://www.nrjetix.com/fileadmin/doc/publications/Lectures_security/Lecture6-1.pdf.

№13 дәріс. **Асимметриялық шифрлердің криптоталдау**

Мақсаты: Асимметриялық шифрлеудің алгоритмдерін криптоталдауға арналған программалық қамтаманы қолдану

Дәріс жоспары:

- Криптоталдау тапсырмаларында ғылыми есептеулерге арналған қолданбалы пакеттерді қолдану
- Программалық құралдар көмегімен асимметриялық шифрлеудің алгоритмдерін криптоталдау
- Қолданылған программалық құралдар жұмыстарын салыстыру

Асимметриялық алгоритмдер өзінің негізінде әлдебір математикалық мәселені қамтығандықтан, Maple, Mathematica, Sage сияқты пакеттерде көптеген белгілі асимметриялық алгоритмдер толығымен іске асырылған. Мұндай іске асырудың мысалдары, мысалы, осы БҚ-ның ресми документацияларында бар. Maple, Mathematica, Sage пакеттері сол себептерге байланысты криптоанализ әдістерін тиімді іске асыруға мүмкіндік береді.

Көптеген бағдарламалау тілдерінде (C/C++, Python), сондай-ақ криптографиялық кітапханаларда осы тілдер үшін факторизация, дискретті логарифмдеу алгоритмдерін және криптоанализдің басқа да әдістерін жүзеге асыру бар. Неғұрлым тиімді әдістерді әзірлеу, сондай-ақ криптоанализ міндеттері үшін есептеу қуаттарын пайдалануды оңтайландыру – бұл әрі қарай зерттеулер үшін ауқымды салалар.

Бақылау сұрақтары мен тапсырмалары

1) Криптографияда қолданылатын математикалық пакеттердегі функцияларды жүзеге асырумен танысу. Қарастырылған пакеттерде криптографиялық алгоритмдерді іске асыру мәніне салыстырмалы талдау жүргізу.
2) Криптоанализдегі математикалық пакеттердің мүмкіндіктерін сипаттау. Бар іске асыруларға шолу жасау.
3) Әртүрлі бағдарламалау тілдерінде криптоанализ әдістерін жүзеге асыру мүмкіндіктерін сипаттау. Салыстырмалы талдау жасау.
Әдебиеттер: [1] – осн., ғылыми-практикалық әзірлемелердің қол жетімді жарияланымдары, интернет материалдары

№ 14 дәріс. **Криптографиялық хэш-функцияларға жасалған криптографиялық шабуылдар, цифрлық қолтаңбалар**
Мақсаты: Криптографиялық хэш-функцияларға жасалған криптографиялық шабуылдарға программалық қамтаманы қолдану, цифрлық қолтаңбалар
Дәріс жоспары:
- Криптоталдау тапсырмаларында ғылыми есептеулерге арналған қолданбалы пакеттерді қолдану
- Программалық құралдар көмегімен асимметриялық шифрлеудің алгоритмдерін, электронды қолтаңбаларды, хэш-функцияларды криптоталдау
- Қолданылған программалық құралдар жұмыстарын салыстыру
- құпия ақпаратты өңдеу процесін автоматтандыру
- оларды жүзеге асырудың алғышарттарын жою арқылы қауіпсіздікке қатер төндіру

Хеш-функциялардың криптоанализі үшін коллизия әдісі қолданылады. Оның мәніне қысқаша тоқталайық. Электрондық-цифрлық қолтаңба (ЭЦҚ) – бұл құжаттың шынайылығына көз жеткізуге, оның авторын анықтауға, құжаттың қол қойылған уақыты мен күнін және т.б. тексеруге мүмкіндік беретін әлдебір ақпарат (функционалдық жиынтық әр түрлі болуы мүмкін). ЭЦҚ криптографиялық хеш-функциямен қалыптастырылатын құжаттың (хабарламаның) криптографиялық бейнесіне негізделгені белгілі.

Электрондық қолтаңба схемаларына шабуылдардың жіктелуін келтіреміз:
- Белгілі ашық кілт негізіндегі шабуыл – шабуылдардың ең әлсізі, қарсыласқа әрдайым қол жетімді;
- Белгілі қол қойылған хабарламалар негізінде шабуыл – қарсыластың иелігінде (M, C) жұптардың кейбір саны бар, мұнда M – әлдебір хабарлама, ал C – оған сәйкес қолтаңба, бұл жерде қарсылас M таңдауына әсер ете алмайды;
- Қол қойылған хабарламаларды таңдау арқылы жасалатын қарапайым шабуыл – қарсылас қол қойылған хабарламалардың кейбір санын таңдай алады, бұл жағдайда ол ашық кілтті осы таңдаудан кейін алады;
- Хабарларды таңдау арқылы бағытталған шабуыл – қол қойылған хабарламаларды таңдау арқылы, қарсылас ашық кілтті біледі;
- Хабарларды таңдауға бейімделген шабуыл – қарсылас ашық кілтті біледі, әрбір келесі қол қойылған хабарды таңдауды алдыңғы таңдалған хабарламаның қол қоюын білу негізінде жасай алады.

Бақылау сұрақтары мен тапсырмалары
1) Криптографияда қолданылатын математикалық пакеттердегі функцияларды жүзеге асырумен танысу. Қарастырылған пакеттерде криптографиялық алгоритмдерді іске асыру мәніне салыстырмалы талдау жүргізу.

2) Криптоанализдегі математикалық пакеттердің мүмкіндіктерін сипаттау. Бар іске асыруға шолу жасау.
3) Кртүрлі бағдарламалау тілдерінде криптоанализ әдістерін жүзеге асыру мүмкіндіктерін сипаттау. Салыстырмалы талдау жасау.
Әдебиеттер: [1] – осн.; ғылыми-практикалық әзірлемелердің қол жетімді жарияланымдары, интернет материалдары, http://www.nrjetix.com/fileadmin/doc/publications/Lectures_security/Lecture6-1.pdf.

№ 15 дәріс. **Заманауи шифрлеу алгоритмдерін криптоталдаудың нәтижелері, оны жүзеге асыру мен жетілдіру мәселелері**
Мақсаты: заманауи криптоталдау саласындағы қолжетімді мақалалар мен нетижелермен танысу, олардың тәжірибелік тұрғыда жүзеге асыру мәселелерін қарастыру
Дәріс жоспары:
- Криптография және криптоталдау саласындағы заманауи мамандардың ашық мақалалары
- Заманауи шифрлердің жарияланған криптоталдау нәтижелерін зерттеу және осы жұмыстарда келтірілген криптошабуылдарды жүзеге асыру мәселелері
-Жарияланған жұмыстардағы заманауи шифрлерге криптографиялық шабуылдарды жүзеге асыру

Қазіргі заманғы белгілі криптографтардың қатарына Bruce Schneier, Eli Biham, Lars Knudsen, Ron Rivest, Claus-Peter Schnorr, Dong-Ho Won, N. Courtois жатады. Толық тізіммен төмендегі ұсынылған көздердегі сілтеме бойынша танысуға болады.

Төменде IACR қауымдастығы (IACR – The International Association for Cryptologic Research) ұйымдастыратын және оның қатысуымен өткізілетін криптография саласындағы конференциялар мен семинарлардың тізімі берілген:

- Crypto, Eurocrypt, Asiacrypt конференциялары;

– TCC, FSE, CHES, PKC, ACNS, INDOCRYPT, RSA Conference, SAC, FOCS, STOC, ICALP, CSS – криптография және қауіпсіздік жүйелері бойынша халықаралық конференция.

N. Courtois және оның бірлескен авторларының жұмыстары қызықты. Оның жарияланымдарымен, сондай-ақ Лондон университетінің криптоанализ бойынша курсында қолданылатын материалдармен (Computer Science Department, University College London) мына сілтемелер бойынша танысуға болады:

- http://www.cs.ucl.ac.uk/students/syllabus_index_2015_16/mscisec/ga18_cryptanalysis/,
- http://blog.bettercrypto.com/?page_id=1368 ескерту.

Басқа маман – Марк Стивенстің материалдары, құралдары және жарияланымдары келесі сілтемелер бойынша қолжетімді:

- hashclash – https://marc-stevens.nl/p/hashclash/,
- http://www.cwi.nl/research/cwi-cryptanalysis,
- https://marc-stevens.nl/research/.

Сондай-ақ, әйгілі Қазақстан математигі, ҚР ҰҒА академигі Мұхтарбай Өтелбаевтың криптография саласындағы еңбектерін атап өтеміз.

NESSIE жобасының сайтында (New European Schemes for Signatures, Integrity, and Encryption) — https://www.cosic.esat.kuleuven.be/nessie/index.html криптография және криптоанализ бойынша әртүрлі материалдар бар, олардың ішінде, мысалы, осы тақырып бойынша қазіргі авторлардың жарияланымдары бар NESSIE public reports.

Мысалы, сайтта қол жетімді "A System for Assisting Analysis of Some Block Ciphers" мақаласында авторлар құрған блоктық шифрларға арналған арнайы бағдарламалау тілі сипатталады. Ол функцияларды (S-box блоктары және "таңдау", раундтар, кілттерді үлестіру үшін арнайы нотациялармен), айнымалылар, константалар, қарапайым арифметика және

екілік сандарға операциялар (AND, OR, XOR, ADD, SUB, MULT, ROL, ROR, SHIFTL, SHIFTR) қамтиды. Мақалада мысал ретінде DES алгоритмін қамтитын программа бар. Сонымен қатар, авторлар "Analyzer" құралын жасаған, ол олар әзірлеген тілді интерпретациялайды және оның көмегімен криптоанализ бойынша белгілі бір жұмыстарды автоматтандырады.

Сондай-ақ сайтта танысу және практикалық қолдану үшін ұсынылатын "Test vectors for all NESSIE candidates" ресурсы бар

Бақылау сұрақтары мен тапсырмалары (еңбек көптігіне байланысты бір тапсырманы таңдап орындауға болады)

1) Қазіргі заманғы криптография саласындағы зерттеулердің нәтижелері туралы баяндама дайындау.

2) Қазіргі криптография саласындағы ғылыми мақалалардың бірімен танысу, баяндама дайындау.

3) Өтелбаевтың криптографиялық алгоритмін зерттеу, баяндама дайындау

Әдебиеттер: [1] – осн. ғылыми-практикалық әзірлемелердің қол жетімді жарияланымдары, интернет материалдары, http://www.nrjetix.com/fileadmin/doc/publications/Lectures_security/Lecture6-1.pdf, криптографтардың жеке беттері – http://www.ekey.ru/info_def/security_library/3, криптография бойынша конференциялар тізімі – https://en.wikipedia.org/wiki/List_of_cryptology_conferences.

Курстық дәріс зерттеу бойынша әдістемелік нұсқаулар

Осы материалды меңгеру барысында көрсетілген әдебиеттерде келтірілген мысалдарға назар аудару керек. Ұсынылған тапсырмаларды өз бетімен меңгеру және орындау барысында тақырып бойынша бақылау сұрақтарына жауап беру керек, келтірілген программалар текстеріне, үлгі есептердің шешулеріне сүйенуге болады