ЎЗБЕКИСТОН АЛОҚА ВА АХБОРОТЛАШТИРИШ АГЕНТЛИГИ

ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ

Ахборот технологиялари факультети

Электрон тижорат кафедраси

Магистратуранинг 5А523601 – “Электрон тижорат” мутахассислиги талабалари учун

«Телекоммуникация тармоқларида ахборот хавфсизлиги»

фанидан тажриба ишларини бажариш бўйича

УСЛУБИЙ КЎРСАТМАЛАР

Тошкент - 2007

Тузувчилар: т.ф.н., проф. Ҳамдамов Р.Ҳ., Ялгашев О.Р.

5А523601 - «Электрон тижорат» магистратура йўналиши “Телекоммуникация тармоқларида ахборот хавфсизлиги” фанидан тажриба ишларини бажариш бўйича бўйича услубий кўрсатмалар.

5А523601 - «Электрон тижорат» магистратура йўналиши “Телекоммуникация тармоқларида ахборот хавфсизлиги” фанидан тажриба ишларини бажариш бўйича бўйича услубий кўрсатмалар Ўзбекистон Республикаси Олий ва ўрта махсус таълим Вазирлиги томонидан 2002 йил 21 февралда 54 – сон буйруқ билан тасдиқланган Давлат таълим стандарти асосида ишлаб чиқилди.

Тақризчилар: Тошкент Ислом Университети табиий фанлар кафедраси мудири, ф.м.ф.н., доцент А.А.Алимов

Тошкент ахборот технологиялари университети Ахборот технологияларининг дастурий таъминоти кафедраси профессори т.ф.д. А.Нишонов

Услубий кўрсатмалар Тошкент ахборот технологиялари университети Ахборот технологиялари факультетининг илмий-услубий кенгашида муҳокама қилинган ва чоп этишга тавсия этилган.

200__ йил «___» _____.____ – сонли баённома

Кириш

Бу услубий кўрсатмаларнинг мақсади “Компьютер тармоқларини ва тизимларини ахборот хавфсизлиги” фани бўйича ўтказилган маъруза дарсларидан олинган назарий билимларни мустаҳкамлаш ҳамда компьютер тармоқларини ахборот хавфсизлигини таъминлаш бўйича тажриба кўникмаларни ҳосил қилиш ва ошириш ҳисобланади.

Ушбу услубий кўрсатмаларда компьютер тизимларига бўлган хужумларни классификациялаш, умумбашарий, корпоратив ва махаллий тармоқларини химоялаш усуллари, ОТ, ТДТ, МБга бўлган хужумлар маъмумотларига эга бўлиш, спамлар ва спамларга қарши чоралар, антивируслар, утилиталар, тармоқларни хиомялаш протоколлари, брандмауэрлар, ва улардан қўлланиш масалалари бўйича тажриба ишлари амалга оширилади.

1 - Тажриба иши

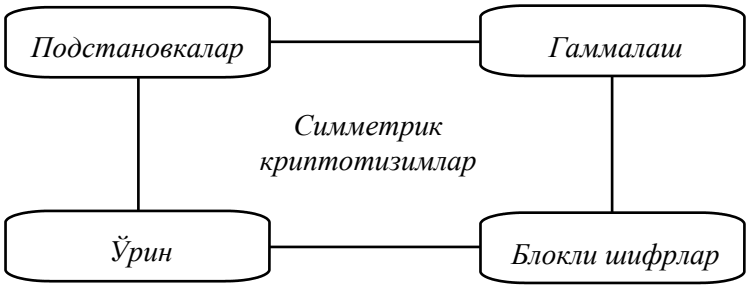
Мавзу: ***Содда шифрлар. Ўрнига қўйиш ва ўрин алмаштириш усулларига асосланган содда криптографик усулларни яратиш ва таҳлил қилиш.***
(2 соат)

Ишнинг мақсади:

Талабаларни шифрлашнинг содда турлари билан таништириш, содда криптографик усуллари яратиш ва таҳлил қилиш кўникмаларини ҳосил қилиш.

Зарурий назарий маълумотлар:

Мавжуд барча криптографик усуллар қуйидаги синфларга ажратилади:



Моно- ва кўп алифболи ўрнига қўйишлар.

Бир хил алифбодан фойдаланган ҳолда очиқ матнни бошқа матнга мураккаб ёки қийин қоида бўйича алмаштириш подстановка ҳисобланади. Юқори криптобардошлиликни таъминлаш учун катта калитлардан фойдаланишга тўғри келади.

Ўрин алмаштиришлар.

Бу ҳам унча мураккаб бўлмаган криптографик акслантириш ҳисобланади, одатда бошқа усуллар билан биргаликда фойдаланилади.

Гамма қўшиш (Гаммалаштириш).

Бу усулда калит асосида генерация қилинадиган псевдотасодифий сонлар кетма-кетлиги очиқ матн устига қўйилади.

Блокли шифрлар.

Блокли шифрлар шифрланадиган матн блокига қўлланиладиган асосий акслантириш усулларини (мумкин бўлган такрорлашлар ва навбатлар билан) тасвирлайди. Блокли шифрлар юқори криптобардошлиликка эга эканлигидан у ёки бу синф акслантиришидан амалда кўпроқ учрайди. Америка ва Россиянинг шифрлаш стандартлари айнан шу синф шифрларига асосланган.

Ўрин алмаштиришлар.

σ ўрин алмаштириш деб $(0,1,...,N-1)$ бутун сонлар тўпламининг қайта тартибланишига айтилади. i бутун сонни i позициядан $\sigma(i)$ позицияга ўтказишда қуйидаги ёзувдан фойдаланамиз:

$$\sigma=(\sigma(0), \sigma(1),..., \sigma(N-1))$$

$(0, 1,...,N-1)$ тўпламда ўрин алмаштиришлар сони $n!=1\cdot2\cdot...\cdot(N-1)\cdot N$ га тенг.

σ га боғлиқ n та элементли $S=\{S_0, S_1,...,S_{N-1}\}$ тўплам киритамиз.

$$\sigma: S \rightarrow S$$

$$\sigma: S_i \rightarrow S_{\sigma(i)},\ 0 \le i < n$$

Бу ерда σ – S тўплам элементлари учун ўрин алмаштиришлар ҳисобланади ва аксинча S автоморфизм $(0, 1, ..., n-1)$ бутун сонларнинг ўрин алмаштиришига мос келади.

Z_m алифбо учун T криптографик акслантиришлар, автоморфизмлар кетма-кетлиги деб номланади: $T=\{T^{(n)}: 1 \le n < \infty\}$

$$T^{(n)}: Z_{m,n} \rightarrow Z_{m,n},\ 1 \le n < \infty$$

Ҳар бир $T^{(n)}$ $Z_{m,n}$ дан олинган n-грамманинг ўрин алмаштирилиши ҳисобланади. $T^{(i)}$ ва $T^{(j)}$ $i \neq j$ ҳолга боғлиқ бўлмаган тарзда аниқланган бўлиши мумкин. n ўлчамдаги очиқ матнни криптографик акслантириш $(m^n)!$ га тенг. Бу m ва n га нопропорционал равишда катталашади: яъни, $m=33$ ва $n=2$ да криптографик акслантириш $1089!$ га тенг. Бу ердан келиб чиқадики, очиқ матн жуда кўп шифрматн каби акслантирилиши мумкин.

Амалда $\{T_k: k \in K\}$ акслантиришли криптографик алгоритмлар жуда кўп параметрларга боғлиқ бўлмаслиги талаб этилади.

Ўрнига қўйиш тизимлари

<u>Таъриф</u>: Z_m алифбода π алмаштириш деб шундай Z_m автоморфизмга айтиладики, бунда t очиқ матннинг ҳарфлари $\pi(t)$ шифрланган матн ҳарфлари билан алмаштирилади:

$$Z_m \rightarrow Z_m;\ \pi: t \rightarrow \pi(t).$$

Барча ўрин алмаштиришлар тўплами, Z_m нинг симметрик гуруҳи дейилади ва келгусида $SYM(Z_m)$ каби белгиланиб олинади.

<u>Тасдиқ</u>: $SYM(Z_m)$ кўпайтириш амали билан гуруҳ ҳисобланади, яъни, бу амал қуйидаги хусусиятларга эга:

1. *Ёпиқлик.* $\pi_1\pi_2$ ўрин алмаштиришларнинг кўпайтмаси $\pi: t \rightarrow \pi_1(\pi_2(t))$ ўрин алмаштириш ҳисобланади.
2. *Ассоциативлик*. $\pi_1\pi_2\pi_3$ кўпайтма натижаси қавслар тартибини ўзгартиришга боғлиқ эмас.
3. *Нейтрал элементнинг мавжудлиги*: $i(t),\ 0 \le t \le m$ каби аниқланадиган i ўрин алмаштириш $\forall\ \pi \in SYM(Z_m)$ учун $i\pi = \pi i$ кўпайтириш амали бўйича $SYM(Z_m)$ нинг нейтрал элементи ҳисобланади.
4. *Тескарисининг мавжудлиги:* $\forall\ \pi$ ўрин алмаштириш учун қуйидаги шартни қаноатлантирувчи фақат битта тескари π^{-1} ўрин алмаштириш мавжуд.

$$\pi\pi^{-1} = \pi^{-1}\pi = i$$

Z_m симметрик гуруҳдаги мумкин бўлган ўрин алмаштиришлар сони $SYM(Z_m)$ нинг тартиби дейилади ва тартиб $m!$ га тенг.

<u>Таъриф</u>. Z_m учун ўрин алмаштириш калити, Z_m симметрик гуруҳ элементларидан ташкил топади.

k калит билан аниқланадиган T_k ўрин алмаштиришлар криптографик акслантиришлар ҳисобланади. Бу акслантиришлар ёрдамида очиқ матннинг $(x_0, x_1, \ldots, x_{n-1})$ n-граммаси шифрланган матннинг $(y_0, y_1, \ldots, y_{n-1})$ n-граммасига ўтказилади.

$$y_i = p(x_i),\ 0 \le i \le n$$

бу ерда n – ихтиёрий сон $(n=1,2,\ldots)$. Агар p, ихтиёрий i $(i=0,1,\ldots)$ да ўзгармас бўлса, T_k моноалифболи ўрин алмаштириш ҳисобланади, акс ҳолда кўп алифболи ўрин алмаштириш дейилади.

<u>Изоҳ</u>. Кўплаб T_k ўрин алмаштиришларга қуйидаги муносабатлар ўринли:

1. Очиқ матннинг ҳар бир белгиси алоҳида шифрланади. $x=(x_0, x_1, \ldots, x_{n-1})$ n-грамма ва унинг $(x_0, x_1, \ldots, x_{S-1})$ префиксини шифрлаш қуйидаги муносабат билан боғланган.

$$T_k(x_0, x_1, \ldots, x_{n-1}) = (y_0, y_1, \ldots, y_{n-1})$$
$$T_k(x_0, x_1, \ldots, x_{S-1}) = (y_0, y_1, \ldots, y_{S-1})$$

2. Шифрланган матннинг y_i ҳарфи фақат p_i калит i-компоненти ва x_i очиқ матннинг i-ҳарфи функцияси ҳисобланади.

Назорат саволлари

1. Ахборот тизимларида криптографик усулларининг аҳамияти?
2. Криптография ва криптология
3. Замонавий криптографиянинг қандай бўлимлари бор?
4. Шифрлаш ва дешифрлаш тушунчалари
5. Шифрлаш ва дешифрлаш терминологияси

6. Симметрик криптотизимлар
7. Криптобардошлилик тушунчаси
8. Криптотизимларга қўйилган талаблар
9. Криптографик усуллар синфлари
10. Очиқ матн тушунчаси
11. Шифрлаш тизимларида калит тушунчаси
12. Ўрнига қўйишлар тизимлари
13. Ўрин алмаштиришлар тизимлари
14. Гаммалаштириш
15. Блокли шифрлар
16. Ўрнига қўйиш тизимларида кўпайтириш амалининг хусусиятлари

Топшириқ вариантлари

1. x_1 ва x_2 сонлар x^2+3x+c тенгламанинг ечими бўлсин (c коэффициентни шундай танлангки, x^2+3x+c тенглама иккита ечимга эга бўлсин). Алифбо таркибида ўзбек алифбосининг бош ҳарфлари киритилган бўлсин. Алифбонинг ҳар бир ҳарфига қуйидаги қонуният билан аниқланадиган сонларни мос қўйиб, "*KRIPTOGRAFIYA*" сўзини шифрлаш, c маълум бўлганда ва маълум бўлмаганда шифрни очиш дастурларини тузинг.

$$f(x) = xx_1^2 + 2xx_2 + 3$$

2. x_1 ва x_2 сонлар x^2+bx+c тенгламанинг ечими бўлсин (b, c коэффициентларни шундай танлангки, x^2+bx+c тенглама иккита ечимга эга бўлсин). Алифбо таркибида ўзбек алифбосининг бош ва кичик ҳарфлари ва бўш жой белгиси киритилган бўлсин. Алифбонинг ҳар бир ҳарфига қуйидаги қонуният билан аниқланадиган сонларни мос қўйиб, "*Ахборот хавфсизлиги*" сўзини шифрлаш, b, c маълум бўлганда ва маълум бўлмаганда шифрни очиш дастурларини тузинг.

$$f(x) = \begin{cases} x^2 x_1, i - жуфт \\ x^3 x_2, i - ток \end{cases}$$

Бу ерда дастлаб $i=0$ бўлиб, алифбонинг ҳар бир белгиси учун биттадан ошади.

3. Алифбонинг ҳар бир белгисига $f(x)=b(x^3+7x^2+3x+a)$ кўпҳад қийматини 7 га бўлиш натижасида ҳосил бўладиган сонни мос қўйиб берилган матнни шифрланг. Бу ерда x – белгининг алифбодаги тартиби, a ва b фиксирланган натурал сонлар.

4. Алифбонинг ҳар бир белгисига $f(x)=b(x^3+7x^2+3x+a)$ кўпҳад қийматини 11 га қолдиқли бўлиш натижасида ҳосил бўладиган сонни мос қўйиб берилган матнни шифрлаш мумкин ёки йўқлигини текширинг. Бу ерда x – белгининг алифбодаги тартиби, a ва b фиксирланган натурал сонлар.

5. Лотин алифбосида матнни шифрлаш икки қадамдан ташкил топган бўлиб, дастлабки қадамда матн ҳарфлари алифбонинг тескари тартибда ҳосил қилинган ҳарфи билан алмаштирилади. Иккинчи қадамда номаълум калитли оддий алмаштириш қўлланилади. Калит маълум бўлмаган ҳол учун очиқ матнни ҳосил қилинг.

6. Шифрлашнинг Цезар усули ва уни очиш алгоритми дастурларини тузинг.

7. Шифрлашнинг Вижинер усули ва уни очиш алгоритми дастурларини тузинг.

8. Шифрлашнинг Вернам усули ва уни очиш алгоритми дастурларини тузинг.

9. Рус алифбосининг ҳар бир ҳарфига қуйидаги жадвал ёрдамида икки рақамдан иборат сонлар мослаштирилган:

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17
Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	
18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	

Олинган рақамли кетма-кетлик ўнгдан чапга уч рақамли қилиб гуруҳларга ажратилди. Сўнгра олинган ҳар бир уч хонали сон 77 га кўпайтирилиб, фақат охирги учта рақами қолдирилди. Натижада қуйидаги қуйидаги равамлар кетма-кетлиги ҳосил бўлди:
317564404970017677550547850355
Очиқ матнни ҳосил қилинг.

10. Инглиз тили алифбосининг бош ҳарфлари (I ва J бир хил бир хил) 5x5 жадвалга ўнгдан чапга, юқоридан пастга тартибда жойлаштирилди. Бу ҳолда аввал *калит сўз* деб номланадиган ҳар хил 6 ҳарфдан ташкил топган сўзлар жойлаштирилди. Сўнгра алифбо тартибида қолган ҳарфлар жойлаштирилди. Бирор сўзни шифрлаш учун жадвалнинг ҳар бир ҳарфини икки рақамли сон билан алмаштирилади. Биринчи рақам – сатр рақами, иккинчиси – устун рақами. Олинган рақамли кетма-кетликни тескари тартибда жойлаштирамиз, сўнгра ҳар бир икки рақамдан ташкил топган сонлар ўрнига ўнгдан чапга ҳосил қилинган жадвалнинг ҳарфлари билан алмаштирамиз. Агар HANDWRITING сўзи PVMTMEDWVAH каби шифрланган бўлса, калит сўзини топинг.

Ишни бажариш тартиби:

1. Лаборатория ишини бажариш учун талабаларга алоҳида компьютер, уларга ўзларига қулай бўлган дастурлаш тилларидан бирида ишлаш имконияти яратилади.
2. Сўралган топшириқлар кетма-кетликда бажарилиб, ишга туширилади.
3. Натижа кутилгандек бўлса қоғозда ва электрон кўринишда ҳисобот тайёрлаш.

Фойдаланилган адабиётлар

1. Баричев С. Махфий бўлмаган криптография.
2. Коробейников А.Г., Гатчин Ю.А. Математические основы криптографии.

Интернет-ресурслар

1. http://works.tarefer.ru/69/100635/index.html
2. http://www.ishodniki.ru/

2 – Тажриба иши

Мавзу: ***Ахборотни ҳимоялаш тизимларида псевдотасодифий сонларни генерация қилиш. Берилган тақсимот қонуни билан тасодифий сонлар датчигининг статистик тавсифини баҳолаш***

Ишнинг мақсади:

Текис ва нормал тақсимланган тасодифий сонлар кетма-кетлигини ҳосил қилиш, қонуниятлар бажарилишини текшириш ва натижаларни керакли мақсадларда ишлата олиш.

Зарурий назарий маълумотлар:

Маълумки /1,2/, агарда (0;1) ораликда текис тақсимланган тасодифий сонлар кетма-кетлиги (ТСКК) мавжуд бўлса, у ҳолда шу кетма-кетлик ёрдамида турли тақсимот қонунларига асосланган тасодифий сонлар кетма-кетлигини моделлаштириш мумкин.

1. (0;1) ораликда текис тақсимланган тасодифий сонлар кетма-кетлигини генерация қилиш масаласини тахлил этамиз.

Текис тақсимланган ТСКК ҳосил қилишга бир нечта алгоритмлар мавжуд /1,2/, шулардан бири қуйидагича:

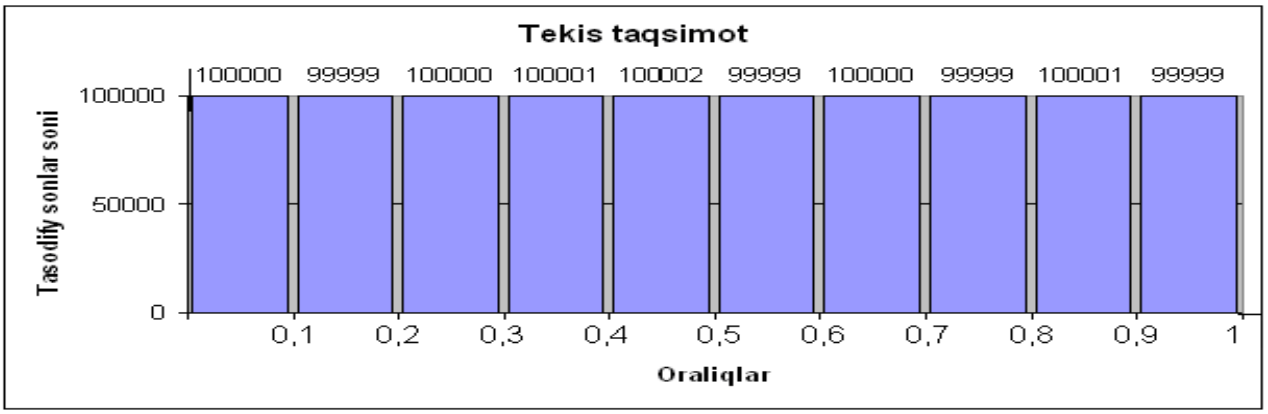
$\nu_i = \{i\ Q\}, \qquad i = 0,1,\ldots,n.$

бу ерда $\{\cdot\}$ амали соннинг каср қисмини ажратиб беради.

Q олдиндан танланган сондир, яъни унинг ўрнида қуйидагилардан бирини олиш мумкин:

$$Q:\left\{\sqrt{2};\ \frac{\sqrt{2}}{2};\ \frac{\sqrt{3}}{3};\ \sqrt{5};\ \frac{\sqrt{5}-1}{2};\right\}.$$

Бу ерда i-нчи элементни ҳосил қилиш учун $i\cdot Q$ нинг ўнлик нуқтадан кейинги қисми олинади. Бундан эса, ҳосил қилинган ТСКК (0;1) ораликда бўлиши таъминланади /1,2/. Ҳосил қилинган элементларнинг такрорланиш шартига текширилганда қуйидаги натижа олинди: 1000000 та элемент генерация қилинганда такрорланиш даври 470837 га(нуқтадан кейин 6 хона олинганда), нуқтадан кейин 7 ва ундан кўп хона олинганда 1000000 та элемент ичида такрорланиш кузатилмади. Бу тақсимотни 1000000 та элементдан иборат графигини чизсак, қуйидагича бўлади:

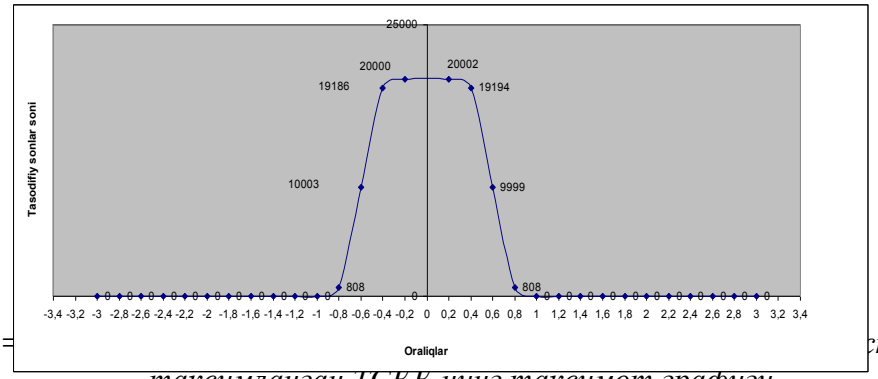


қийматлар йиғиндисининг тақсимот қонуни нормал тақсимотга интилади /1,2/. Ьундан, $n \geq 0$ ва эҳтимоллиги p>0.95 билан ҳосил қилинган тақсимотни нормал дейилади /1,2/.

(0;1) ораликда текис тақсимланган тасодифий сонлар кетма-кетлигидан нормал тақсимланган ТСКК ни генерация қилиш учун қуйидаги формуладан фойдаланилади:

$$\eta_j = \sum_{i=1}^{12} \nu_i - 6 \quad , \qquad j=0,1,\ldots,n.$$

Бу тақсимот қонунини такрорланиш шартига текширсак, қуйидаги натижага эга бўламиз: 100000 та элемент генерация қилинганда такрорланиш даври 19615 га (нуқтадан кейин 6 хона олинганда), 100000 та элемент генерация қилинганда нуқтадан кейин 7 ва ундан кўп хона олинганда 1000000та элемент ичида такрорланиш кузатилмади. Бу тақсимотни 100000 та элементдан иборат графигини чизсак, қуйидагича бўлади:



2- расм. (m= ...сперсия, нормал тақсимланган ТСКК нинг тақсимот графиги.

Ҳозирги кунда криптография соҳасида ТСКК дан фойдаланиш яхши самара беради. Шифрлашда ТСКК дан фойдаланиш криптоаналитикка қандайдир қонуниятларни бериши қийин. Яъни шифрматнни очишда криптоаналитик шифрлаш қонуниятига эга бўлиши мураккаб жараён ҳисобланади. Криптографияда бир марталик дафтарча (блокнот), DES алгоритми, калитлар генерация қилиш, гаммалаштириш ва бошқа алгоритмларни қўллаш жараёнида турли тақсимотли тасодифий сонларни ҳосил қилиш зарурияти туғилади.

Назорат саволлари

1. Тасодифий сонлар тушунчаси
2. ТСККга қўйиладиган талаблар
3. ТСКК алгоритмлари
4. ТСКК тақсимот қонуниятлари
5. Текис тақсимот
6. Нормал тақсимот
7. Экспоненциал тақсимот
8. Логнормал тақсимот
9. ТСКК берувчи датчиклар
10. ТСКК бардошлилиги
11. ТСККнинг қўлланилиш соҳалари

Топшириқ вариантлари

1. Текис тақсимланган қонуният асосидаги ТСКК дастурини тузинг.
2. Нормал тақсимланган қонуният асосидаги ТСКК дастурини тузинг.
3. Экспоненциал тақсимланган қонуният асосидаги ТСКК дастурини тузинг.
4. Логнормал тақсимланган қонуният асосидаги ТСКК дастурини тузинг.
5. Текис тақсимланган қонуният асосидаги ТСКК дастурини тузинг ва 1000000 та қиймат генерация қилиб, такрорланиш даврини топинг.
6. Нормал тақсимланган қонуният асосидаги ТСКК дастурини тузинг ва 10000 та қиймат генерация қилиб, такрорланиш даврини топинг.
7. Текис тақсимланган n - ўлчамли сферада тасодифий векторларни ҳосил қилиш дастурини тузинг. Бу ерда $\xi_i = \frac{\eta_i}{\sqrt{\sum_{i=1}^{n} \eta_i^2}}, \xi = (\xi_1, .\xi_2, ..., \xi_n)$ – тасодифий вектор.
8. Нормал тақсимланган қонуният асосидаги ТСКК дастурини тузинг ва графигини чизинг.

9. $\xi = (\xi_1, .\xi_2, ..., \xi_n)$ – тасодифий вектор элементлари йиғиндиси 1 га тенг эканлигини текширинг.

10. Текис ва нормал тақсимланган ТСККлар учун янги алгоритм ўйлаб кўринг ва унинг дастурини тузинг.

Ишни бажариш тартиби:

1. Лаборатория ишини бажариш учун талабаларга алоҳида компьютер, уларга ўзларига қулай бўлган дастурлаш тилларидан бирида ишлаш имконияти яратилади.
2. Сўралган топшириқлар кетма-кетликда бажарилиб, ишга туширилади.
3. Натижа кутилгандек бўлса қоғозда ва электрон кўринишда ҳисобот тайёрлаш.

Фойдаланилган адабиётлар:

1. Голенко Д.И. Моделирование и статистический анализ последовательности псевдослучайных чисел на ЭЦВМ. -М.: Наука,1965.
2. Коробейников А. Г, Ю.А.Гатчин. Математические основы криптологии. Учебное пособие. СПб: СПб ГУ ИТМО, 2004.

Интернет-ресурслар

1. www.ishodniki.ru
2. www.wikipedia.org

3 - Тажриба иши

Мавзу: ***RSA алгоритми дастурини яратиш (2 соат)***

Ишнинг мақсади: Талабаларни ҳозирги вақтда кенг ишлатилаётган ассимметрик криптоалгоритмлар билан таништириш ва буни мисолидаги реализациясини кўриш.

Зарурий назарий маълумотлар:

RSA алгоритми 1977 йилда Рона Риверс, Ади Шамир ва Леонардо Эдельман томонидан яратилган ва уларнинг исмларидан келиб чиқиб номланган.

Бунда ҳисоблаш нуқтаи назаридан катта туб сонларни генерация қилиш осон, аммо катта сонни туб кўпатувчиларга ажратиш амалда мумкин эмаслигидан фойдаланилган. RSA криптотизимининг очилиш мураккаблиги катта сонни туб кўпайтувчиларга ажратишга тенг кучли эканлиги амалда исботланган (Рабин теоремаси).

Ассимметрик алгоритмлар:

Икки томон ўзаро махфий хабар алмашиши учун, ёпиқ калит уларнинг бири томонидан генерация қилиниши ва ёпиқ канал орқали иккинчи томонга узатилиши керак. Яъни, умумий калит тақсимланишнинг ўзи алоҳида криптотизим талаб қилади.

Буни ҳал қилиш учун классик ва замонавий алгебрадан олинган натижалар асосида **очиқ калитли криптотизимлар** ёки **ассимметрик** таклиф этилди.

Бунда ахборот тизимининг ҳар бир томонидан ўзаро маълум қонуният орқали боғланган калит яратилади. Калитлардан бири **очиқ** бошқаси эса **ёпиқ** ҳисобланади. Очиқ калит публикация қилинади ва уни адресатга хат жўнатмоқчи бўлган барча олиши мумкин. Ёпиқ калит эса сир сақланади.

Очиқ матн адресат очиқ калити билан шифрланади ва адресатга узатилади. Шифрматнни қайта ўша очиқ калит билан очиш мумкин эмас. Дешифрлаш фақатгина адресатнинг ўзигагина маълум бўлган ёпиқ калит билан амалга оширилиши мумкин.

Очиқ калитли криптотизимлар бир томонлама ёки тескариси мавжуд бўлмаган функциялардан фойдаланилади. Бундай функциялар қуйидаги хусусиятга эга: берилган *x* қиймат учун *f(x)* қиймати нисбатан осон ҳисобланади. Аммо *y= f(x)* берилган бўлса x ни ҳисоблашнинг осон усули мавжуд эмас.

Тескариси мавжуд бўлмаган функциялардан тўплами турли хилдаги очиқ калитли криптотизимлар яратишга олиб келади, аммо хар қандай тескариси мавжуд бўлмаган функцияни хам амалиётда қўллаш мумкин эмас.

Яъни, *тескариси мавжудмас* деганда, назарий жихатдан мавжудмаслиги эмас, балки замонавий ҳисоблаш воситаларини ишга солиб, амалда чекли вақт орлиғида ҳисоблаб бўлмаслиги тушунилади.

Шу сабабли очиқ калитли тизимлар мустаҳкамлиги (ОКТ) таъминлаш учун уларга қуйидаги иккита асосий талаб қуйилади:

1. Очиқ матнни қайта ишлаш жараёни *ўгирилмас* бўлиши ва очиқ калит асосида матнни қайта тиклаш эҳтимоли йуқотилиши лозим.
2. Замонавий технологиялар даражасида ОК асосида ёпиқ топилмаслиги керак. Бу билан бир қаторда шифрни очиш мураккаблиги (амаллар миқдори) аниқ қуйи бахоси берилиши керак.

RSA алгоритмининг математик асослари:

Теорема 1. *Ферма кичик теоремаси.*

Агар p –туб сон бўлса, p билан ўзаро туб бўлган ҳар қандай x учун

$x^{p-1} = 1 (\text{mod}\quad p)$ (1) ва $x^{p} = x (\text{mod}\quad p)$

ўринли.

Исбот. (1) ва (2) ларни $X \in Z^{p}$ учун исботлаш етарли. Исботлашни индукция усулида олиб борамиз.

(2) тенглама $\alpha = 0$ ва $\alpha = 1$ учун ўринли эканлиги маълум. Бундан

$$x^{p} = (x-1+1)^{p} = \sum_{0 \le j \le p} C(p, j)(x-1)^{j} = (x-1)^{p} + 1 (\text{mod}\quad p)$$

$0 < j < p$ учун $C(p, j) = 0 \ (\text{mod}\quad p)$ эканлигидан ва юқорида айтилганлар асосида индукция методи теорема тўғрилигини тасдиқлайди.

Таъриф: Эйлер функцияси $\varphi(n)$ деб, n дан кичик ва n билан ўзаро туб бўлган бутун мусбат сонлар миқдорига айтилади.

n	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
$\varphi(n)$	**1**	**2**	**2**	**3**	**2**	**6**	**4**	**6**	**4**	**10**	**4**

Теорема 2. Агар $n = p \cdot q$ бўлса, (p ва q бир-биридан фарқли туб сонлар), унда $\varphi(n) = (p-1)(q-1)$ ўринли.

Теорема 3. Агар $n = p \cdot q$, (p ва q бир-биридан фарқли туб сонлар) ва x сони p ва q билан ўзаро туб бўлса у ҳолда

$x^{\varphi(n)} = 1 \ (\text{mod}\quad n)$ ўринли.

Натижа: Агар $n = p \cdot q$ бўлса, (p ва q бир-биридан фарқли туб сонлар) ва e - $\varphi(n)$ билан ўзаро туб бўлса, у ҳолда $E_{e,n} : x \to x^{e} (\text{mod}\quad n)$ алмаштириш Z_n да бир қийматли алмаштириш бўлади.

Яна шу маълумки, агар e - $\varphi(n)$ билан ўзаро туб бўлса, шундай d -бутун сон топиладики, унда

$e \cdot d = 1 \ (\text{mod}\quad \varphi(n))$ (3)

ўринли бўлади.

RSA алгоритмидаги қадамлар кетма-кетлиги:

$n = p \cdot q$ бўлсин, бунда p ва q бир-биридан фарқли туб сонлар, e ва d учун (3) шарт бажарилса, у ҳолда $E_{e,n}$ ва $E_{d,n}$ алмаштиришлар Z_n да инверсиялар бўлиб ҳисобланади. e, d, p, q маълум бўлганда худди $E_{e,n}$ каби $E_{d,n}$ ни топиш ҳам осон

ҳисобланади. Агар e ва n лар маълум, лекин p ва q номаълум бўлса, у ўолда $E_{e,n}$ бир томонлама функция ҳисобланади; берилган n учун $E_{d,n}$ ни топиш n ни туб кўпайтувчиларга ажратиш билан баробар. Агар p ва q етарлича катта туб сон бўлса, у ҳолда n ни туб кўпайтувчиларга ажратиш амалда мумкин эмас. Худи мана шу хусусият RSA шифртизим асосини ташкил этади.

i - фойдаланувчи p_i ва q_i туб сонлар жуфтлиги ни танлайди, $n_i = p_i \cdot q_i$ ва $\varphi(n_i)$ билан ўзаро туб бўлган (R_i, d_i) сонлар жуфтлигини ҳисоблайди. Очиқ маълумотлар доскасида $\{(e_i, n_i)\}$ очиқ калитлар эълон қилинади.

Масалан, $X = (x_0 x_1, \dots, x_{n-1}), \quad x \in Z_n, \quad 0 \le i < n$ нинг аввал n_i асосга кўра кўриниши олинади:

$N = c_0 + c_{in_i} + \dots$

i - *фойдаланувчи* матнни j фойдаланувчига узатишда n га E_{d_i,n_i} алмаштиришни бажариб, матнни j фойдаланувчига узатишда шифрлайди:

$N = E_{d_i,n_i} \quad n = n'$

j *фойдаланувчи* E_{e_i,n_i} дан фойдаланиб n' дешифрлашни амалга оширади.

$\mathrm{N}' \to E_{e_i,n_i} \quad n' = E_{e_i,n_i} \cdot E_{d_i,n_i} \quad n = n$

Маълумки, E_{e_i,n_i} га нисбатан E_{d_i,n_i} *инверсияни* топиш учун $n = p_i \cdot q_i$ кўпайтувчиларни билиш керак бўлади.

Энг яхши алгоритмлардан фойдаланиб $n = 10^{100}$ учун туб кўпайтувчиларга ажратиш замонавий технологиялар имкониятларидан ташқарида ҳисобланади.

RSA алгоритми тадбиқи:

Ҳозирги кунда RSA алгоритми мустақил криптографик маҳсулот (масалан PGP дастурида) ва кенг тарқалган дастурларнинг бир қисми сифатида реализация қилиниб келинмоқда (Microsoft ва NetScape комнанияларининг Интернет броузерларида). Бунга мисол қилиб SSL, S-HTTP, S-MIME, S/WAN, STT ва PCT каби стандартларни айтиш мумкин.

Назорат саволлари:

1. Ассимметрик криптотизимларга таъриф беринг.
2. Қандай функцияга тескариси мавжудмас функция дейилади?
3. RSA алгоритмида очиқ ва ёпиқ калитлар қандай боғланган?
4. Очиқ калитли тизимлар мустаҳкамлигини таъминлаш учун уларга қандай талаблар қуйилади?
5. Ферма теоремасига нимани тасдиқлайди?
6. Берилган бутун сон асосида эйлер функцияси қандай қиймат қайтаради?
7. RSA қандай вазифанинг мураккаблигига асосланади?
8. RSA алгоритми қандай дастурларда ишлатилган?

Топшириқ вариантлари:

1. RSA алгоритмини реализация қилинг

Ишни бажариш тартиби:

4. Лаборатория ишини бажариш учун талабаларга алоҳида компьютер, уларга ўзларига қулай бўлган дастурлаш тилларидан бирида ишлаш имконияти яратилади.
5. Сўралган топшириқлар кетма-кетликда бажарилиб, ишга туширилади.

6. Натижа кутилгандек бўлса қоғозда ва электрон кўринишда ҳисобот тайёрлаш.

Фойдаланилган адабиётлар

3. Баричев С. Махфий бўлмаган криптография.
4. Коробейников А.Г., Гатчин Ю.А. Математические основы криптографии.

Интернет-ресурслар

3. http://works.tarefer.ru/69/100635/index.html
4. http://www.ishodniki.ru/

4 - Тажриба иши

Мавзу: *Diffie-Hellman алгоритмига асосланган симметрик калит алмашиш протоколини ишлаб-чиқиш ва дастурини яратиш.*

Зарурий назарий маълумотлар:

Диффи ва Хэллман очиқ калитли криптотизимлар учун *дискрет даражага ошириш* функциясини таклиф қилишди.

*Ўгирилмаслик*нинг (необратимость) олдини олиш *p* элементдан ташкил топган Галуа чекли майдонида даражали функциянинг осон ҳисобланиши билан таъминланади (бу ерда *p* -исталган туб сон ёки ҳар қандай даражали туб сон). Бундай майдонларда логарифмни ҳисоблаш жуда қийин ҳисобланади.

Агар $y=\alpha^x$, $1<x<p-1$ бўлса, бу ерда x – *GF(p)* майдоннинг фиксирланган элементи, бунда *GF(p)* да $x=log_\alpha y$. *x* га эга бўла туриб, *y* ни осон ҳисоблаш мумкин. Бунинг учун *2 ln(x+y)*та кўпайтириш амали бажарилади.

Тескари масала, яъни *y* асосида *x* ни ҳисоблаш қийин бўлади. Агар *p* етарлича тўғри танланган бўлса, унда логарифмни чиқариб олиш қуйидаги ҳисоблашларга пропорционал бўлади:

$L(p) = exp\ \{ (\ln p\ \ln\ln p)^{0.5} \}$

Ахборот алмашиш учун А абонент *1..p-1* оралиғидаги x_1 тасодифий сонни танлайди. Бу сонни махфий калит сифатида сақлайди ва Б абонентга қуйидаги сонни юборади:

$y_1 = \alpha^x \bmod p$

Худди шундай тарзда *Б* абонент x_2 танлаб, y_2 ни ҳисоблайди ва *А* абонентга юборади. Натижада улар $k_{12} = \alpha^{x1^{x2}} \bmod p$ ни ҳисоблашлари мумкин. k_{12} ни ҳисоблаш учун А абонент y_2 ни x_1 даражага кўтаради. Б абонент ҳам худди шундай йўл тутади. Шу тарзда иккала абонентда ҳам оддий шифрлаш алгоритмларда фойдаланиш мумкин бўлган умумий k_{12} калит ҳосил бўлади. RSA алгоритмидан фарқли равишда, бу алгоритмни шифрлашда ишлатиб бўлмайди.

Учинчи шахс x_1 ва x_2 ларни билмай туриб, y_1 ва y_2 лар асосида k_{12} ни ҳисоблашга уриниши мумкин. Бу муаммо дискрет логарифмларни ҳисоблаш муаммоси билан эквивалент бўлиб, бу очиқ калитли тизимларда саволлигича қолмоқда. Ҳозирги кунда эса бунга оддий ечим топилмаган. Агар 1000-битли туб сонни ҳосил қилишга 2000 та амал бажариш керак бўлса, тескари масалага (Галуа майдонида логарифмни ҳисоблаш) 10^{30} та амал бажариш керак бўлади.

Кўриниб турибдики, Диффи-Хэллман алгоритмининг қанчалик оддий эканлигига қарамасдан RSA алгоритмидан фарқли равишда унинг иккинчи камчилиги, калитни очишда кафолатланган паст баҳосининг йўқлигидир.

Бундан ташқари, бу алгоритм махфий калит алмашишга имкон берсада, аутентификация масаласини таъминламайди. Қўшимча воситаларсиз абонентлардан бири калитларни айнан ўзига керакли абонент билан алмашганига ишонч ҳосил қила олмайди.

Калитларни тақсимлаш тўғрисида айтилганларга хулоса сифатида қуйидагиларни айтиш мумкин. Калитларни бошқариш масаласи қуйидагиларни таъминлай оладиган калитларни тақсимлаш протоколини излашга олиб келади:

- калитларни тақсимлаш марказини рад этиш имконияти;
- сеанс иштирокчиларининг ҳаққонийлигини биргаликда тасдиқлаши;
- сеанс ишончлилигини дастурий ёки аппаратли воситаларни ишлатиш орқали сўров - жавоб механизми билан тасдиқлаш;

калит алмашишда минимал миқдорда ахборот алмашиш.

Назорат саволлари

1. Дискрет даражага ошириш функцияси
2. Ўгирилмаслик (необратимость) тушунчаси
3. Очиқ ва калит тушунчалари
4. Диффи-Хеллман алгоритми ёрдамида калит алмашиш жараёни
5. Диффи-Хеллман алгоритмининг камчиликлари
6. Диффи-Хеллман алгоритмида аутентифакция масаласи
7. Калитларни тақсимлаш протоколлари

Топшириқ вариантлари

1. Диффи-Хеллман алгоритми ёрдамида калит абонентлар ўртасида калитлар алмашиш жараёнининг дастурини тузинг

Ишни бажариш тартиби:

1. Лаборатория ишини бажариш учун сервер компьютер, талабаларга алоҳида компьютер, уларга ўзларига қулай бўлган дастурлаш тилларидан бирида ишлаш имконияти яратилади.
2. Икки фойдаланувчи ўртасида калит алмашиш жараёни ташкиллаштирилади.
3. Сўралган топшириқлар кетма-кетликда бажарилиб, ишга туширилади.
4. Натижа кутилгандек бўлса қоғозда ва электрон кўринишда ҳисобот тайёрлаш.

Фойдаланилган адабиётлар

1. Алферов А.П. Основы криптографии.
2. Баричев С.Г., Серов Р.Е. "Основы современной криптографии"

5 – Лаборатория иши

Мавзу: ***Хабарнинг рақамли дайджестини ҳисоблаш алгоритмини ишлаб чиқиш ва дастурини яратиш.***

Ишнинг мақсади:

Мавжуд хеш-функцияларни ўрганиб чиқиш, уларни таҳлил қилиш ва бир-бири билан солиштириш.

Зарурий назарий маълумотлар:

Хеш функция - ихтиёрий узунликдаги М-ахборотни фиксирланган узунликга сиқиш ёки иккилик саноқ системасида ифодаланган маълумотларни фиксирланган узунликдаги битлар кўринишидаги қандайдир комбинацияси (сверткаси) деб аталувчи функциядир/1,2/. Криптографияда хеш функциялар қуйидаги масалаларни ечиш учун қўлланилади:

- берилган ахборотларни узатиш ва сақлашда уларнинг тўлалигини назорат қилиш;
- берилган маълумот аутентификациясини таъминлаш учун.

Юқорида келтирилган фикр мулоҳазаларни математик формаллаштирамиз:

Х-барча маълумотлар тўплами бўлсин;

Y-фиксирланган узунликдаги векторлар тўплами бўлсин.

У ҳолда қуйидагича таъриф ўринли:

Хэш-функция деб, ҳар қандай h: $X \to Y$ осон ҳисобланувчи ва $\forall$ M –ахборот учун h(M) = H фиксирланган узунликга эга бўлган функцияга айтилади/1,2,3/.

Криптографияда хеш функцияларни ҳисоблаш учун бир неча алгоритмлар мавжуд. Масалан, MD2, MD4, MD5, SHA-1, SHA-2, SHA-512 ва бошқалар.

Шу алгоритмлардан энг кенг тарқалгани ва АҚШ стандарти деб тан олинган SHA оиласига мансуб алгоритмларга тўхталамиз. SHA(Secure Hash Standard) – Хавфсиз хеш алгоритми, АҚШнинг Технологиялар ва Стандартлар Миллий Институти (NIST) томонидан ишлаб чиқилган. SHA-1 алгоритми узунлиги 2^{64} дан кичик бўлган кирувчи ахборотни 160-битли фиксирланган кўринишдаги чиқувчи ахборот кўринишига ўтказиб беради. Ўз навбатида бу чиқувчи ахборот Рақамли Имзо Алгоритми (Digital Signature Algorithm) учун кирувчи ахборот сифатида қўлланилади/4/..

Бу алгоритмни хавфсиз (secure) дейилишига сабаб, худди шундай қийматли фиксирланган кўриниш берувчи ахборотни топиш, ёки бир хил хеш қиймат берувчи 2та хар хил ахборотни топиш мумкин эмаслигидадир. Транзит пайтида ахборотга исталган ўзгартириш киритиш унинг хеш қийматини ўзгартириб юборади/2,4/. Ҳар доим янги алгоритм топилса, албатта уни криптотаҳлил қилинади. SHA-1 алгоритми ҳам криптотаҳлил қилинган ва натижаси ижобий бўлган. Масалан, 2005 йил бошида Рижмен ва Освальдлар SHA-1 ни 2^{80}та операция билан коллизияга(бир хил хеш қиймат берувчи 2та хар хил ахборот) учратиш мумкинлигини топишган. 2005 йил февралида эса Xiaoyun Wang, Yiqun Lisa Yin, ва Hongbo Yu лар 2^{69} та топишган. Ва ниҳоят, 17 август 2005 йилда Xiaoyun Wang, Andrew Yao ва Frances Yao лар 2^{63}та операцияда коллизияга учрашини исболашган/2/. Шундан сўнггина NIST 4 та янги хеш функция ўйлаб чиқди. Бу функциялар умумий қилиниб, SHA-2 оиласи деб юритилади. Уларнинг фарқи фиксирланган узунликдадир, яъни улар берадиган хеш-қиймат турли узунликда бўлади. Мос равишда бу функциялар SHA-224, SHA-256, SHA-384 ва SHA-512 деб номланган.

SHA-1 да 5 та хар хил 32-битли 16 лик саноқ системаси кўринишидаги ўзгарувчилар ишлатилар зди. Натижада улар ҳаммаси қўшилиб, бир ўзгарувчига ўзлаштирилар эди ва 160-бит кўринишдаги фиксирланган узунликка олиб келинар зди. SHA- 224 да 8 та ўзгарувчи ишлатилади, натижада 8-ўзгарувчи ташлаб юборилади ва 224 бит кўринишдаги фиксирланган узунлик олинади. SHA-256 да ҳам 8 та 32-битли ўзгарувчи ишлатилади, лекин натижа учун ҳаммаси олинади. SHA-512 да 8 та 64-битли ўзгарувчи ишлатилади. SHA-384 да ҳам 8 та 64-битли ўзгарувчи ишлатилади, лекин фиксирланган узулик учун 7- ва 8- ўзгарувчилар ташлаб юборилади/4/. Қуйида бўш тўплам учун хеш қийматларни кўрамиз.

SHA1("") = da39a3ee 5e6b4b0d 3255bfef 95601890 afd80709

SHA256("") = e3b0c442 98fc1c14 9afbf4c8 996fb924 27ae41e4 649b934c a495991b 7852b855

SHA512("") = cf83e135 7eefb8bd f1542850 d66d8007 d620e405 0b5715dc 83f4a921 d36ce9ce
47d0d13c 5d85f2b0 ff8318d2 877eec2f 63b931bd 47417a81 a538327a f927da3e

Бу қийматлар NIST томонидан расмий тарзда текширилган. SHA-2 ҳам криптотаҳлил қилинган, лекин натижа бўлмаган, яъни коллизияга учраш эҳтимоли ҳозирча йўқ.

SHA алгоритмлари DSA билан биргаликда e-mailда, электрон тўлов ўтказмаларида, рақамли имзо ва ахборот тўлалигини талаб қиладиган дастурий таъминотларда, маълумотларни сақлашда ишлатиш мумкин.

Назорат саволлари

1. Хеш функция тушунчаси
2. Хеш функция ва хеш қийматнинг фарқи
3. Хеш функцияларга қўйиладиган талаблар
4. Хеш функцияларнинг қўлланилиш соҳалари
5. MD оиласи тўғрисида маълумот беринг
6. SHA оиласи тўғрисида маълумот беринг
7. Snefru алгоритми тўғрисида маълумот беринг
8. ГОСТ Р 34.11.94 алгоритми тўғрисида маълумот беринг
9. MD ва SHA оиласига мансуб алгоритмларнинг ўхшашлик томонлари
10. MD ва SHA оиласига мансуб алгоритмларнинг асосий фарқлари
11. MD5 га оид криптотаҳлиллар
12. SHA-1 га оид криптотаҳлиллар

Топшириқ вариантлари

1. SHA-1 хеш функциясининг дастури тузинг ва “китоб” сўзи хеш қийматини олинг/4/.
2. SHA-224 хеш функциясининг дастури тузинг ва “университет” сўзи хеш қийматини олинг.
3. SHA-256 хеш функциясининг дастури тузинг ва 1000000та символ учун хеш қийматини олинг.
4. SHA-384 хеш функциясининг дастури тузинг ва бўш хабар учун хеш қийматини олинг.
5. SHA-512 хеш функциясининг дастури тузинг.
6. MD2 хеш функциясининг дастури тузинг ва 3 хил мураккабликдаги хабарлар учун хеш қийматлар олинг.
7. MD4 хеш функциясининг дастури тузинг.
8. MD5 хеш функциясининг дастури тузинг.
9. SHA-1 хеш функциясига ўзингиз ўзгартириш киритиб, дастурини тузинг ва ўзгартиришларни асослаб беринг.
10. Snefru алгоритми дастурини тузинг ва SHA-1 билан солиштириб кўринг, ҳар хил хабарлар учун текшириб кўринг.

Ишни бажариш тартиби:

1. Лаборатория ишини бажариш учун талабаларга алоҳида компьютер, уларга ўзларига қулай бўлган дастурлаш тилларидан бирида ишлаш имконияти яратилади.
2. Сўралган топшириқлар кетма-кетликда бажарилиб, ишга туширилади.
3. Натижа кутилгандек бўлса қоғозда ва электрон кўринишда ҳисобот тайёрлаш.

Фойдаланилган адабиётлар:

1. Коробейников А. Г, Гатчин Ю.А - Математические основы криптографии. Питер,2004
2. Брюс Шнайер - Прикладная криптография(2-е издание).

3. Курьязов Д.М. - Сонлар назарияси элементларининг ассимметрик криптотизимлар асосларида қўлланишлари.

Интернет-ресурслар

1. www.nist.gov

6 - Тажриба иши

Мавзу: ***Рақамли имзо алгоритмини ишлаб чиқиш. (3 соат)***

Ишнинг мақсади: Талабаларни ҳозирги вақтда электрон ҳужжат алмашинуви, интернет тўловлар ва умуман матнни таркиби ўзгармагани ва шахсни идентификация қилиш воситаси сифатида кенг ишлатилаётган электрон рақамли имзо билан таништириш ва асосий хусусиятларини ўрганиш.

Зарурий назарий маълумотлар:

Кириш:

Одатда, исталган хат ёки хужжат остига жавобгар шахс ёки масъул ходим шахсий имзоси қўйилади. Бу қуйидаги икки мақсадни кўзлайди. Биринчидан қабул қилувчи ўзида бор имзо нусхалари билан таққослаб хатнинг ҳаққонийлигини тасдиқласа, иккинчидан шахсий имзо хужжат муаллифлигини тасдиқловчи юридик асос бўлади.

Электрон рақамли имзонинг асосий хусусиятлари :

Замонавий электрон ҳужжатларнинг турли кўринишларида ва уларни қайта ишлаш воситаларининг кўпчилигида муаллиф ҳаққонийлигини таъминлаш муаммосига дуч келинади.

Очиқ калитли криптотизимлар маълумотлар аутентификациясини таъминлай олмайди. Бу функцияни таъминлаш учун криптографик комплексларда маълумотлар аутентификацияси воситасини қўшиш керак.

Муаллифликни инкор қилиш. Александр Борисга хабар жўнатгани ҳолида, ҳеч қандай хабар жўнатмаганлигини билдиради.

Ўзгартириш. Борис Александрдан олган хабарни ўзгартиради ва уни шундайлигича қабул қилганлигини билдиради.

Қалбакилаштириш. Борис Александрдан олган хабар мазмунини ўзгартиради ва хабар айнан шу кўринишда жўнатилганлигини билдиради.

Актив ҳужум. Владимир Александр ва Борис ўртасида алмашинаётган маълумотларни ўзгартириш мақсадида ўзлаштириб олади.

Маскировка (имитация) – Воҳид Бобурга Алишер номидан хабар жўнатади.

RSA алгоритмига асосланган рақамли имзо

Кўриб ўтган RSA алгоритми оддий ва шу билан бирга энг кўп тарқалган электрон усули ҳисобланади. Қуйида унга мисол кўрамиз. Бундан ташқари ўнлаб схемалардаги рақамли имзо усуллари мавжуд.

Фараз қиламиз

d,p,q - ёпиқ, e, $n=pq$ – эса очиқ калитлар

Изоҳ:

1. n туб кўпайтувчиларга ажратилса: $\varphi(n)=(p-1)(q-1)$ олинади. $\varphi(n)$ ва e ни била туриб d ни топиш мумкин.

2. e ва d га эга бўлиб эса $\varphi(n)$га карали сонларни билиш мумкин, бу карралилар n нинг бўлувчиларини топиш имконини беради.

Масалан, “DATA” Александрдан Борисга узатиладиган хабар бўлсин. Александр хабарни Борисга жўнатишдан олдин имзолайди, яъни

$$Ee_B,n_B\{Ed_A,n_A\{DATA\}\}.$$

ни бажаради.

Бунинг учун у қуйидаги калитлардан фойдаланилади.

- Александрнинг ёпиқ калити Ed_A,n_A дан
- Бориснинг очиқ калити Ee_B,n_B дан

Борис хабарни ўқиш учун аввал ўз ёпиқ калитлари Ed_B,n_B дан фойдаланиб

$$Ed_A,n_A\{DATA\} = Ed_B,n_B\{Ee_B,n_B\{Ed_A,n_A\{DATA\}\}\}$$

га эга бўлади. Сўнгра Александр очиқ калити Ee_A,n_A дан фойдаланиб

$$DATA = Ee_A,n_A\{Ed_A,n_A\{DATA\}\}.$$

олади ва натижада Александр жўнатган “DATA” хабарини тиклайди.

Юқоридаги схема бир қанча бузилишлар олдини олади.

Александр ёпиқ калити фақатгина унинг ўзига маълум бўлганлигидан муаллифликни инкор эта олмайди.

Учинчи шахс ёпиқ калитни билмаганлиги сабабли хабар мазмунини ҳам билолмайди ва унга ўзгартириш ҳам кирита олмайди.

Схема кўпгина муаммоли вазиятларни бошқа шахслар аралашувисиз ҳам ҳал қилишга имкон беради.

Баъзида маълумотларни шифрламасдан, уларга фақатгина электрон имзо қўйиш талаб этилади. Бундай ҳолатларда матнининг ўзи жўнатувчи ёпиқ калити билан шифрланади ва шифрлаш натижасида олинган символлар кетма-кетлиги матн остига ёзилади. Қабул қилувчи матннинг остки ёзувини муаллиф очиқ калити билан қайта очиб, натижани матн билан солиштиради.

Назорат саволлари:

1. Электрон рақамли имзо қандай вазифаларни бажаради?
2. Очиқ калитли криптотизимлар қандай камчиликка эга?
3. Муаллифликни инкор қилиш хусусияти.
4. Ўзгартириш хусусияти.
5. Қалбакилаштириш хусусияти.
6. Актив ҳужум.
7. Маскировка хусусияти.
8. RSA алгоритмига асосланган рақамли имзо алгоритмнинг қандай хусусиятига асосланади?.
9. Электрон рақамли имзонинг бошқа схемасига мисол келтиринг.

Топшириқ вариантлари:

1. RSA алгоритмига асосланган рақамли имзо алгоритмини амалга оширинг

Ишни бажариш тартиби:

7. Лаборатория ишини бажариш учун талабаларга алоҳида компьютер, уларга ўзларига қулай бўлган дастурлаш тилларидан бирида ишлаш имконияти яратилади.
8. Сўралган топшириқлар кетма-кетликда бажарилиб, ишга туширилади.
9. Натижа кутилгандек бўлса қоғозда ва электрон кўринишда ҳисобот тайёрлаш.

Фойдаланилган адабиётлар

1. Баричев С. Махфий бўлмаган криптография.
2. Коробейников А.Г., Гатчин Ю.А. Математические основы криптографии.

Интернет-ресурслар

1. http://works.tarefer.ru/69/100635/index.html
2. http://www.ishodniki.ru/

МУНДАРИЖА