## БЕХАТАРИИ ТРАНЗАКСИЯҲО

**Бехатарии иттилоотӣ.** Асоси мавҷудияти тиҷорати электрониро дар Интернет усулҳои таъминоти бехатарии иттилоотии транзаксияҳо дар шабака ташкил мекунанд. Мафҳуми “бехатарии иттилоотӣ”-ро ҳамчун вазъи устувори низомҳои иттилоотӣ аз таъсирҳои эҳтимолӣ ва мақсаднокро меноманд, ки таваккали маҳвшавӣ, тағйирёбӣ ва дуздии иттилоотро, ки ба корбар ё молики иттилоот зарар мерасонад, пешгирӣ менамояд. Дастрасии иттилоот дар шабака барои корбарони ихтиёрӣ озод аст, бинобар ҳамин ҳам саҳми усулҳои ҳифзи иттилоот дар шабака хеле ҳам бузург арзёбӣ мегардад.

Мувофиқи тадқиқотҳои омории гузаронидашуда, яке аз монеъаи асосӣ дар рушди тиҷорати электронӣ ин хавфи харидорон ба эътимоднокии воситаҳои харидуфурӯш дар Интернет ба ҳисоб меравад. Омилҳои зерин ба рушди тиҷорати электронӣ тавассути кортҳои кредитӣ мусоидат намекунанд:

- *Кафолати нокифояи иттилооти шахсӣ (маҳрамона)*. Хавф ва хатари аз тарафи шахсони бегона дастрас намудани иртиботи иттилоот ва аз он ҷудо карда гирифтани иттилооти зарурӣ. Масалан, иттилоот оиди кортҳои кредитӣ ва ғайра;

- *Сатҳи нокифояи санҷиши аниқи муайянкунии иштирокчиёни амалиётҳо*. Харидор ҳангоми ташрифи мағозаи электронӣ ба эътимоднокии ширкати пешниҳоднамудаи молу хизматрасониҳои шубҳа доштанаш мумкин аст. Фурӯшанда бошад, дар навбати худ наметавонад дарҳол молики аслии корти кредитӣ будани харидорро муайян намояд;

- *Кафолати нокифоя ба дурустии додаҳо*. Ҳангоми иртиботи иттилооти комилан дуруст шахсони сеюм метавонанд ғайриқонунӣ ин иттилоотро дастрас намуда, дар шакли нодурӯст пешниҳод намоянд.

Барои таъмини сатҳи зарурии таваккали транзаксияҳо дар Интернет усулҳои *рамзгузорӣ*, *имзои рақамӣ* ва *шаҳодатномаҳои электронӣ* истифода мешаванд.

**Рамзгузорӣ.**

Барои амалисозии харидуфурӯши шабакавӣ дар навбати аввал боварӣ ҳосил намудан лозим аст, ки иттилоотӣ шахсӣ барои афроди шахсони бегона комилан дастнорас аст. Бинобар ин, дар харидуфурӯш тавассути Интернет аз технологияи рамзгузорӣ истифода мебаранд. Ҳангоми тадбиқи технологияи рамзгузорӣ матни муқаррарӣ ба шакли махсусе табдил дода мешавад, ки онро бе истифодабарии калиди махсусӣ рамзкушоӣ хондан ғайри имкон мегардад. Кашфи чунин технология иртиботи бехавфи иттилоотиро ба Интернет тавассути хатҳои дастраси умумӣ мусоидат намуд.

Низомҳои дилхоҳи рамзгузорӣ аз рӯйи методологияи муайян кор ва фаъолият мекунад. Он аз як ё якчанд алгоритмҳои рамзгузорӣ (формулаҳои математикӣ), калидҳои барои истифодабарии алгоритими рамзкушоӣ ва инчунин низомҳои идоракунии калидҳо иборат мебошад. Мувофиқи методологияи рамзгузорӣ дар аввал ба матн алгоритми рамзгузорӣ тадбиқ гардида, баъдан калид сохта мешавад, ки бо ёрии он матни рамзбандишударо кушодан имконпазир мегардад. Матни рамзбандигардида ба ҷои лозимӣ тавассути шабака интиқол дода мешавад ва барои ҳосил намудани матни аввала айнан ҳамин алгоритми рамзхонӣ истифода бурда мешавад. Ба методологияи рамзбандӣ инчунин *равандҳои сохтани калидҳои рамзхонӣ ва паҳнкунии онҳо* шомил мешаванд.

Яке аз алгоритмҳои маъмул ва паҳнгардидаи рамзбандии иттилоот ин алгоритми муттаҳидсозии калид бо матн мебошад.

Амнияти ин намуд низомҳои рамзбандӣ танҳо аз махфӣ будани калиди рамзкушоӣ, ки дар алгоритми рамзбандӣ истифода шудааст вобаст аст, на аз махфигии худи алгоритм. Алгоритмҳои зиёди рамзбандӣ ба ҳамагон дастрасанд ва бинобар ин, онҳо озмудашуда ва эътимоднок ба ҳисоб мераванд.

Лекин масъалаи асосии ин усулҳо аз бехатарии равандҳои ҳосилкунӣ ва паҳнкунии калидҳои рамзкушоӣ ва рамзбандӣ ба иштирокчиёни алоқамандӣ, иборат мебошад.

Дар ҳоли ҳозир ду намуди асосии алгоритмҳои криптографӣ[1] ба меъёрҳо ва стандартҳо ҷавобгӯ мавҷуданд:

- *Алгоритмҳои классикӣ* ё *симетрӣ* дар асоси истифодабарии калидҳои махфии пушида ё пинҳонӣ бунёд шудаанд ва дар ҳоли тадбиқи онҳо амалҳои рамзбандӣ ва рамзкушоӣ бо як калид анҷом дода мешаванд;

- *Алгоритмҳо бо калиди кушода*. Дар ин алгоритмҳо як калид барои рамзбандӣ ва як калиди дигар барои рамзкушоӣ истифода мешаванд. Чунин усули рамзгузориҳоро алгоритмҳоро *асимметрӣ* мегӯянд.

Барои ҳалли масъалаҳои паҳнкунии калидҳо бо усули симметрии рамзбандӣ дар асоси натиҷаҳои бо роҳи классикӣ ва алгебраи муосир ба даст омада, *системаҳо бо калидҳои кушода* ё *системаҳои криптографии асимметрӣ* пешниҳод гардидаанд. Моҳияти ин усулҳо аз он иборат аст, ки ба ҳар як суроға ду калид тавлид (генератсия) карда мешавад, ки бо ҳамдигар аз рӯйи қоидаи муайян алоқамандӣ доранд. Ҳарчанд ҳар як ҷуфти калидҳо ҳам барои рамзбандӣ ва ҳам барои рамзкушоӣ иттилоот мувофиқат менамояд, калиди дар рамзбандӣ истифода шуда барои рамзкушоӣ дубора истифода нашуда, барои рамзкушоӣ аз калиди дуюм истифода мебаранд. Як калид кушода эълон карда шуда калиди дуюм бошад

[1] Криптография аз забони юнонӣ kryptos – махфӣ, сир ва grapho - менависам. Мактуби шартан махфӣ, махфинавис.

пӯшида аст. Калиди кушода озод аст ва барои корбарони ихтиёрӣ дастрас буда метавонанд ба суроғаҳои зарурӣ пайғому мактубҳои рамзбандишударо ирсол намоянд. Калиди дуюм бошад махфӣ нигоҳ дошта мешавад. Матни ибтидоӣ бо калиди кушода рамзбанди гардида ба суроға ирсол мегардад. Матни рамзбанди шуда дубора бо калиди кушода рамзкушоӣ намегардад. Рамзкушоии иттилоот танҳо бо калид пӯшида амалӣ мегардад, ки он танҳо ба қабулкунандаи иттилоот маълум асту халос.

Низомҳои криптографӣ бо калиди кушода ҳамчун *равандҳои бебозгашт* ё *функсияҳои яктарафа* истифода бурда мешаванд.

Алгоритмҳои рамзгузорӣ бо калидҳои кушода дар системаҳои муосири иттилоотӣ ба таври васеъ мавриди баҳрабардорӣ қарор гирифтаанд. Якчанд низомҳои криптографӣ бо калидҳои кушода маълуманд. Яке аз системаҳои дар ҳоли ҳозир нисбатан муваффақ ин системаи *RSA* мебошад, ки ҳануз соли 1978-ум пешниҳод гардида буд. Алгоритми RSA аз рӯйи ҳарфҳои аввали насаби муаллифони он номгузорӣ гардида аст: R.L. Rivest, A. Shamir ва L. Adleman. Ин алгоритм амалан дар стандарти ҷаҳонӣ барои системаҳои кушода тадбиқи худро ёфтааст ва аз тарафи Кумитаи машваратии байналмилалии телефонӣ ва телеграфӣ (КМБТТ) тавсия дода шудааст.

**Имзои рақамӣ.**

Иттилооти рамзбандигардидаи тавассути шабакаи саросарии Интернет интиқол меёбад ва рамзбандӣ имконият медиҳад, ки он аз таъсири шахсони бегона ҳифз гардад. Лекин барои бехатарии пурра ва боварӣ ҳосил намудан ба эътимоднокии шахсияти иштирокчии дуюми транзаксия, ки ба ӯ дар ҳақиқат ҳам иттилоот пешбинӣ шудааст, рамзбандии иттилоот кифоя нест. Дар тиҷорат яке аз омилҳои ниҳоят муҳими муайянкунии шахсияти фармоишдиҳанда ин имзои

муайянкунандаи шахсия ба шумор меравад. Дар тиҷорати электронӣ низ ҳаммаънои имзои маъмулӣ (муқаррарӣ), *имзои электронӣ* ё *имзои рақамӣ* ба таври васеъ истифода мешавад. Бо ёрии имзои рақамӣ исбот намудан мумкин аст, ки транзаксия аз тарафи манбаъи муайян шинохта гирифта шуда ва дар раванди иртибот иттилоот зарар ва талафот наёфтааст. Ба мисли технологияи рамзбандӣ дар технологияи имзои рақамӣ низ ё калиди кушода (дар ин маврид ҳар ду иштирокчӣ аз як калид истифода мебаранд) ва ё калиди махфӣ (дар ин ҷо бошад аз ҳар ду калидҳои кушода ва махфӣ истифода мебаранд) баҳрабардорӣ мегарданд. Дар ҳоли ҳозир барои истифодабарӣ бештар аз технологияи калиди кушода ба монанди RSA истифода мебаранд.

Ҳангоми муайянкунии асли шахсияти ирсолкунанда, калидҳои кушода ва махфии истифодагардида таъсири мутақобил доранд, чунки онҳо ҳангоми рамзбандӣ аллакай истифода шуда буданд. Зеро дар технологияи рамзгузорӣ калиди кушода барои рамзбандӣ ва калиди махфӣ барои рамзкушоӣ истифода мешавад. Дар вақти муайянкунии асли шахсият бо ёрии имзои рақамӣ бошад, баръакс. Ба ғайр аз ин, имзои рақамӣ кафолати ягонагӣ ва аслӣ будани пайғомро муайян мекунад. Имзои рақамӣ имконияти иттилоотро аз чашми шахсони бегона пинҳон ё ҳифз карданро надоранд. Барои ҳамин ҳам алгоритмҳои рамзбандӣ пешбинӣ гардидаанд. Масалан, технологияи стандартии санҷиши аслӣ будани санадҳои электронӣ DSS (Digital Signature Standard – стандарти имзои рақамӣ)-ро дар ИМА ширкатҳое истифода мебаранд, ки бо ташкилотҳои давлатӣ ҳамкорӣ доранд. Инчунин истифодабарӣ аз технологияи RSA имкониятҳои хеле зиёдро ба корбарон мусоидат менамояд. Ин ба он вобаста аст, ки ин технология ҳам дар муайянкунии имзои рақамӣ ва ҳам дар рамзгузории иттилоот якбора истифода мешавад. Имзои рақамӣ имконият медиҳад, ки шахсияти аслии равонкунандаи иттилоот муайян карда шавад. Ин технология дар асоси истифодабарии калиди шахсии муаллифи ирсолкунандаи иттилоот бунёд гардидааст ва ҳади аз ҳама зиёди амнияти

иттилоотиро дорад.

Дар мамлакатҳои ғарб ҳоли ҳозир аз имзои рақамӣ дар ҳуҷҷатгузориҳои давлатӣ, тиҷоратӣ, иҷтимоӣ ва ғайра ба таври васеъ истифода мебаранд. Қайд кардан зарур аст, ки яке аз унсурҳои асосии ҳукуматҳои электрониро имзои рақамӣ ташкил мекунад.

**Шаҳодатномаҳои рақамӣ.**

Чи тавре пештар қайд намудем, яке аз масъалаи асосии низомҳои криптографӣ ин паҳнкунии калидҳо ба ҳисоб меравад. Дар ҳолати истифодабарии усулҳои симметрии рамзгузорӣ ин масъала ниҳоят ҷидӣ мебошад, бинобар ҳамин дар рамзгузории иттилоот барои интиқоли калидҳо бо воситаи Интернет, зиёдтар аз усулҳои асимметрии (нобаробар) рамзгузорӣ баҳрабардорӣ менамоянд.

Усулҳои асимметрӣ барои архитектураи кушодаи Интернет нисбатан мувофиқанд. Лекин дар ин ҳолат ҳам истифодабарии калидҳои кушода ҳифзи иловагии мувофиқатро барои муайянкунии иртибот бо калиди махфӣ талаб мекунад. Бе ҳифзи иловагӣ шахсони номаълум ё зараррасон худро соҳиби имзои рақамӣ муаррифӣ намуда ба тиҷорати электронӣ халал ворид карда онро ба низоми ноустувор мубаддал менамоянд. Дар ин ҳолатҳо ҳар як нафар метавонад худро ба ҷои нафари дигар пешниҳод намояд. Ҳамаи ин масъалаҳо ба зарурати санҷиш ё озмоиши калиди кушод оварда мерасонад. Барои ҳалли чунин масъалаҳо аз шаҳодатномаҳои электронӣ ё рақамӣ истифода мебаранд.

*Шаҳодатномаи электронӣ* гуфта санади рақамиеро мегӯянд, ки калиди кушодаро ба корбар ё замимаи мушаххас алоқаманд месозад. Барои ба шаҳодатномаи электронӣ эътимод кардан аз имзои рақамии электронӣ истифода бурда мешавад, ки он аз тарафи Маркази шаҳодатномадиҳии электронӣ тасдиқ гардидааст. Вобаста аз вазифаҳояш, Маркази шаҳодатномадиҳии электронӣ ягона

сохтор барои калидҳои кушода ба ҳисоб меравад (PKI – Public Key Infrastructure). Калидҳои кушодаи Маркази шаҳодатномадиҳии электрониро истифода карда корбари ихтиёрӣ метавонад ба дурустӣ ва эътибори шаҳодатномаи электронии Маркази шаҳодатномадиҳии электронтро санҷад ва мазмуни онро истифода намояд. Барои ба шаҳодатномаи электронӣ бовар ва эътимод намудан ташкилотҳои ихтиёрии бонуфуз вазифаи Марказҳои шаҳодатномадиҳии электрониро иҷро менамоянд. Дар ҳоли ҳозир яке аз манбаи маъруф ва эътимодноки шаҳодатномаҳои электронӣ ин ширкатҳои Thawte (www.thawte.com) ва VeriSign (www.verisign.com) мебошанд. Инчунин дигар системаҳои шаҳодатномадиҳӣ ба монанди World Registry (IBM), Cyber Trust (GTE) ва Entrust (Nortel) мавҷуданд.

Технологияи шаҳодатномаҳои рақамӣ аз рӯйи алгоритми зерин кор мекунад. Барои истифодабарии шаҳодатнома, харидори имкониятдор бояд аз манбаи боэътимоди шаҳодатномадиҳӣ онро харидорӣ намояд. Барои харидории шаҳодатномаи электронӣ ба ӯ зарур аст, ки санадҳои тасдиққунандаи шахсият, ҳуҷҷатҳои зарурӣ ва нусхаи калиди кушодаро тибқи талаботҳои пешниҳоднамудаи Маркази шаҳодатномадиҳии электронӣ ба сомонаи манбаи шаҳодатномадиҳӣ тариқи электронӣ пешниҳод намояд. Баъд аз соҳиби шаҳодатномаи электронӣ гардидан, корбар имконият пайдо мекунад, ки бо воситаи Интернет харидории мол ва хизматрасониҳои гуногунро фармоиш дода, имзои рақамӣ ва нусхаи шаҳодатномаи электрониро замима намояд. Шӯъбаи хизматрасонии муштариёни ширкатҳои пешниҳодкунандаи мол ва хизматрасониҳо тавассути Интернет, фармоишро қабул мекунад ва аз шаҳодатномаи электронӣ истифода карда шахсияти харидорро муайян намуда, дурустии калиди кушодаро аниқ мекунад.

Қайд намудан зарур аст, ки технологияи шаҳодатномаҳои электронӣ дусамта (дуҷониба) амал мекунанд. Ин маънои онро дорад, ки на танҳо ширкат дурустии фармоиш ва шахсияти харидорро муайян карда метавонад. Инчунин харидор низ дар

навбати худ имконият дорад, ки тариқи шаҳодатномаи электронии худ ба эътимоднокии ширкати пешниҳодкунандаи молу маҳсулот боварӣ ҳосил намуда, баъдан мол ва хизматрасониро харидорӣ намояд.

Баъд аз он ки тарафҳо эътимоднокии санҷиши якдигарро мегузаронанд, метавонанд амалиёти харидуфурӯшро амалӣ намоянд. Ҳар як иштирокчии харидуфурӯш ба калидҳои кушоди якдигар боварӣ ҳосил намудаанд ва метавонанд иттилооти иртиботшавандаро рамзгузорӣ намоянд ва ба онҳо имзои рақамӣ гузоранд. Чунин механизм эътимоднокии харидуфурӯшро ба сатҳи баланд бардошта тарафҳо масъулияти дар назди худ гузоштаро иҷро мекунанд.

**Саволҳо:**

1. Бехатарии иттилоотӣ чист?
2. Кадом омилҳо ба рушди тиҷорати электронӣ монеъа эҷод мекунанд?
3. Барои бехатарии иттилоотӣ дар Интернет аз кадом усулҳо истифода мебаранд?
4. Криптография чист?
5. Кадом алгоритмҳои криптографиро медонед?
6. Таъиноти имзои рақамӣ ва шаҳодатномаҳои электронӣ аз чӣ иборат аст?