**3-маъруза. Симметрик шифрлаш алгоритмидан фойдаланиб калит узатиш протоколлари**

**Режа:**

1. Шамир протоколи.
2. Нидхем-Шрёдер протоколи.
3. Wide-Mouth Frog протоколи.
4. Yahalom протоколи.
5. Отвей-Риис протоколи.
6. Neuman-Stubblebine протоколи.
7. Ньюман-Стабблайн протоколи.
8. SKID протоколи.

**Симметрик криптотизимларга асосланган калитларни тақсимлаш протоколлари**

Ушбу маърузада симметрик шифрлаш алгоритми ёрдамида генерация қилинган калитни алмашиш протоколлари кўриб чиқилади. Бу протоколларда ахборот алмашинуви субъектлари бўлган *А* ва *B* фойдаланувчилар умумий - калитга эга деб қабул қилинади. Бу протоколлар, учинчи ишончли томоннинг иштирок этиши ёки этмаслигига боғлиқ равишда икки турга бўлинади. Аввало учинчи ишончли томон иштирок этмаган протоколларни кўриб ўтилади. Бунинг учун қуйидаги белгилашлар киритилади:

Е – шифрлаш алгоритми;

 – вақт белгиси;

 – *А* -фойдаланувчининг тасодифий сони;

 – *А* -фойдаланувчининг генерация қилиш тартиб рақами;

*В* – B -фойдаланувчининг идентификацион рақами;

– иккала томонга ҳам маълум бўлган калит.

Симметрик калитли криптотизимда фойдаланувчилардан ташқари калитларни тарқатувчи томон, яъни калитларни тарқатиш маркази ҳам иштрок этади. Симметрик криптотизим ёрдамида калитларни алмашиш протоколи қуйидагича амалга оширилади:

1. А - фойдаланувчи В - фойдаланувчи билан алоқа ўрнатиш учун калит тарқатувчига мурожаат қилади ва сеанс калитини сўрайди.

2. Калит тарқатувчи сеанс калитни генерация қилади ва бу калитини икки нусхада шифрлаб, А - фойдаланувчига узатади.

3. А - фойдаланувчи ўзига тегишли шифрланган сеанс калитини дешифрлайди.

4. А - фойдаланувчи шифрланган сеанс калитининг иккинчи нусхасини В фойдаланувчига узатади.

5. В - фойдаланувчи ўзининг шифрланган калитини дешифрлайди.

6. А ва В - фойдаланувчилар маҳфий алоқа учун юқорида ҳосил қилинган сеанс калитидан фойдаланадилар.

Бу протоколда сеанс калитлар тарқатувчини ишончли томон деб қабул қиладилар. Агар криптоаналитик актив ҳужум ёрдамида ёки бошқа қандайдир усул билан сеанс калитларини қўлга киритса, у ҳолда криптоаналитик алоқа тармоғига уланиб, тармоқдаги барча алмашинувчи маҳфий маълумотларни кузатиш ёки эшитиш имкониятига эга бўлади.

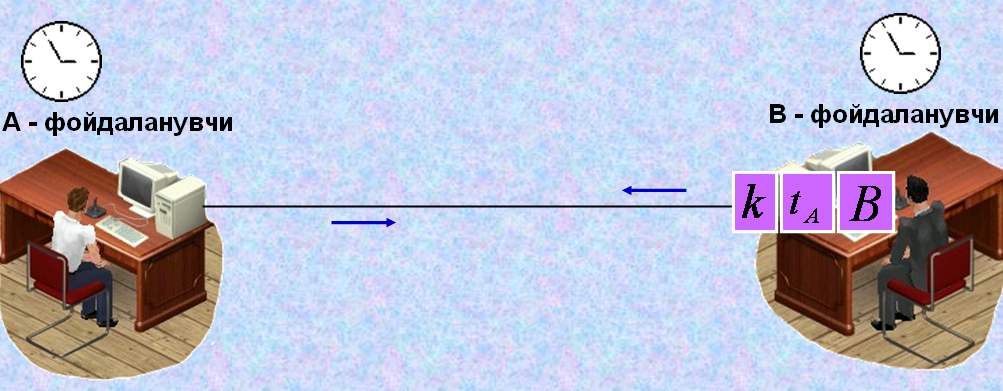
Юқорида баён қилинган тизимнинг яна бир камчилиги шундаки, ҳар бир калит алмашишда қатнашувчи учинчи томон, яъни калитларни тарқатиш маркази, мазкур тизимнинг нозик нуқтаси ҳисобланади. Агар унда бирор камчилик кузатилса, бутун тизимга таъсир этади. Қуйида шу каби бир нечта протоколлар ҳақида тўхталиб ўтилади.

**1 – протокол**

Симметрик шифрлаш алгоритми ёрдамида генерация қилинган калитни узатиш протоколининг содда кўриниши – сеанс калитини бир раундда узатиш. Бутун протокол ягона маълумотдан ташкил топган:

A → В: .

В - фойдаланувчи умумий калит ёрдамида бу маълумотни дешифрлайди. Бу ҳолда **** - сеанс калит вазифасини бажаради [2]



**Хулоса**

Агар кўриб чиқилган протоколда:

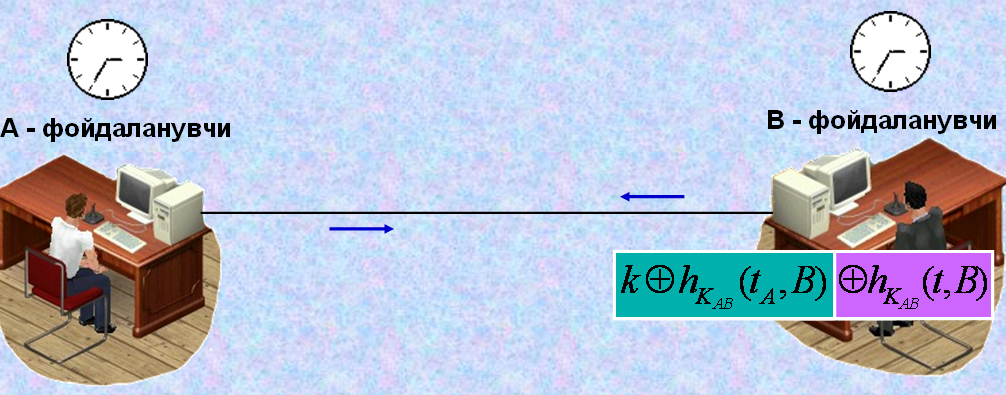
1. Bақт белгиси узатилмаса, криптоаналитик айнан шу маълумотни қайта узатиши мумкин.

2. В - фойдаланувчининг идентификацион рақами кўрсатилмаса, криптоаналитик бу маълумотни *А-*фойдаланувчининг ўзига узатиши мумкин ва натижада *А -*фойдаланувчи маълумот В -фойдаланувчидан келган ёки келмаганлигини аниқлай олмайди.

3. Сеанс калит  функция ёрдамида ҳисоблаб топилиши мумкин. Агар  функция сифатида бир томонлама функциядан фойдаланилса, томонларнинг ҳеч бири натижавий калитни назорат қила олмайди.

Юқорида келтирилган протоколда шифрлаш алгоритми ўрнига калит ёрдамидаги хэш - функциядан фойдаланиш мумкин:

А → В: .

В -фойдаланувчи маълумотни қабул қилади. У ҳам калит орқали хэшлаш функциясини билади. Қабул қилган маълумотидан вақт белгисини ажратиб олади. Унинг кейинги вазифаси вақт белгиси ва ўзининг идентификация рақамини бирлаштириб калитли хэш - функция ёрдамида хэшлашни амалга ошириш. Чиққан  натижани қолган  маълумотга XOR амали бўйича қўшилади. Натижада  - сеанс калит ҳосил бўлади. 

Агар тизим умумий синхрон вақтга эга бўлмаса, лекин калитнинг янгилигига ишонч ҳосил қилиш талаб қилинса, у ҳолда вақт белгисини тартиб рақам билан алмаштириш мумкин. У ҳолда протокол қуйидаги кўринишга келади:

**2 – протокол**

В - фойдаланувчи ўзининг  -тасодифий сонини ҳосил қилиб уни А-фойдаланувчига узатади:

В → A : 

А - фойдаланувчи бу тасодифий сонни қабул қилиб, унга ўзи ҳосил қилган сеанс калитини ва В - фойдаланувчининг идентификация рақамини бирлаштириб иккала фойдаланувчи учун умумий бўлган калит ёрдамида шифрлайди ҳамда В - фойдаланувчига узатади:

A → В: .

В - фойдаланувчи  ва В ни текшириб,  -сеанс калитининг тўғри эканлигига ишонч ҳосил қилади. Хэш - функциядан фойдаланилса протоколнинг кўриниши қуйидагича бўлади:

В → A : 

A → В: .

Ушбу протоколни шундай ўзгартириш мумкинки, натижада -сеанс калитини бир томон эмас, балки иккала томон биргаликда генерация қиладилар [2].

А ва В -фойдаланувчилар  ва  -сонларидан бошқа тасодифий  ва  - сонларни генерация қиладилар. Бу ерда  ва  - сонлари калит материаллари сифатида фойдаланилади,  ва  -сонлари эса калитнинг янги калит эканлигини таъминлайди. У ҳолда протокол қуйидагича амалга оширилади:

1) юқорида келтирилган протокол каби В -фойдаланувчи ўзининг - тасодифий сонини А -фойдаланувчига узатади:

В → A :  ;

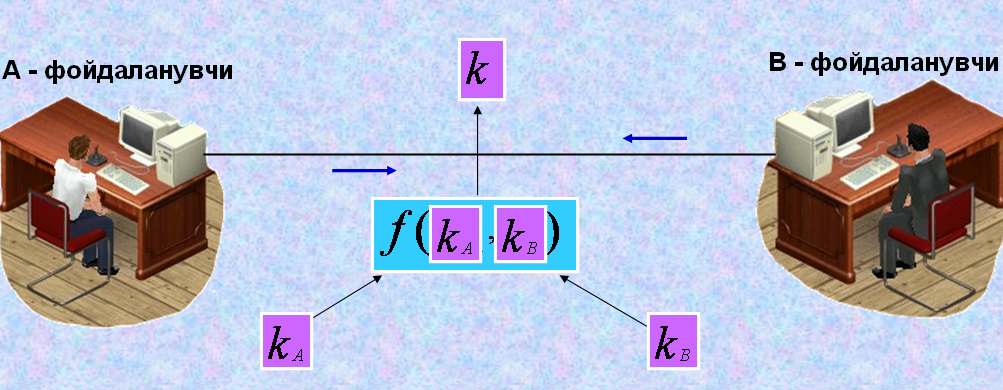
2) А -фойдаланувчи бу тасодифий сонни қабул қилади. Ўзаро аутентификацияни таъминлаш ҳамда сеанс калитни биргаликда хосил қилиш учун қуйидаги маълумотни В -фойдаланувчига узатади:

A → В: ;

3) В -фойдаланувчи маълумотни дешифрлаб,  -тасодифий сонни текширади. Натижа тўғри бўлса, А -фойдаланувчига  - ни умумий калит билан шифрлаб узатади:

В → A: ;

4) Натижада ҳар бир томон умумий калитни олдиндан келишиб олинган бирор функция ёрдамида  қонуният билан ҳисоблаб топиши мумкин.



Қуйида эса  **Шамир протоколи** деб аталувчи (калитсиз) умумий маҳфий маълумотдан фойдаланмаган ҳолда калитни узатиш протоколини кўриб чиқилади. Бу протокол қадамларига мувофиқ калитнинг маҳфийлик масаласи таъминланади.

Шундай шифрлаш ва дешифрлаш ўзгартиришлари мавжудки барча *х* -маълумотлар,  ва  -калитлар учун қуйидаги шарт бажарилади:

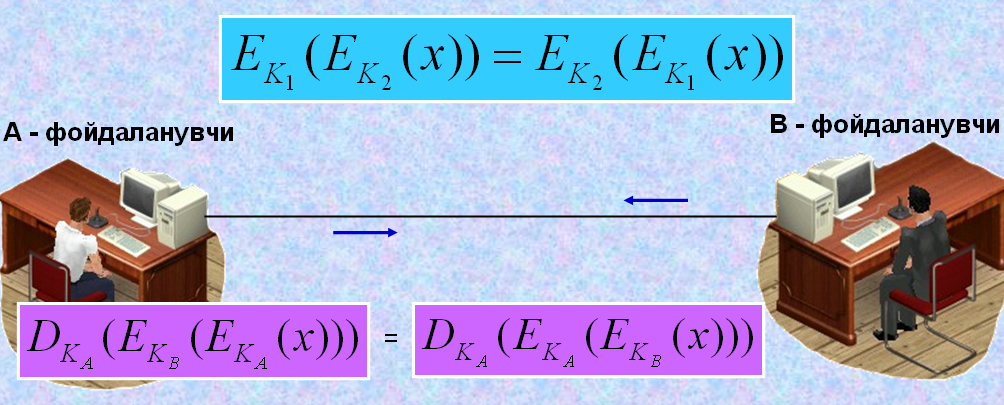
.

У ҳолда А ва В -фойдаланувчилар  -сеанс калитини узатувчи қуйидаги 3 - босқичли протколдан фойдаланишлари мумкин:

(1) A → В: 

(2) В → A : 

(3) A → В: .



Хусусан, Шамир протоколида модуль бўйича даражага кўтариш амалидан фойдаланиш таклиф этилган, яъни . Шундай қилиб, бу протоколнинг криптобардошлиги дискрет логарифмлаш масаласининг мураккаблигига асосланган. Шамир протоколининг камчилиги шундаки, бу протоколда аутентификация масаласи ҳал этилмаган.

**Нидхем-Шрёдер протоколи**

Рожер Нидхем ва Михаэл Шрёдерлар томонидан яратилган бу протоколда арбитр ва симметрик криптотизимдан фойдаланилади:

1. А - фойдаланувчи ишончли томонга (W) ўзининг исмини, В-фойдаланувчининг исмини ва ўзининг тасодифий сонини узатади.

A → W :  .

2. 3 - ишончли томон сеанс калитни генерация қилади. Бу сеанс калитни ва А - фойдаланувчининг исмини В - фойдаланувчи билан умумий бўлган калит орқали шифрлайди. Сўнгра А -фойдаланувчи ва ўзи учун умумий бўлган калит ёрдамида А - фойдаланувчининг тасодифий сони, В- фойдаланувчининг исми, калит ва шифрматнни шифрлайди. Ниҳоят у шифрланган маълумотни А -фойдаланувчига узатади:

W → В :  .

3. А - фойдаланувчи маълумотни дешифрлаб,  -калитни олади. У  ва 1 - босқичда узатилган  ни солиштиради. Сўнгра А - фойдаланувчи ишончли томон шифрлаган маълумотни В -фойдаланувчига узатади:

A → В :  .

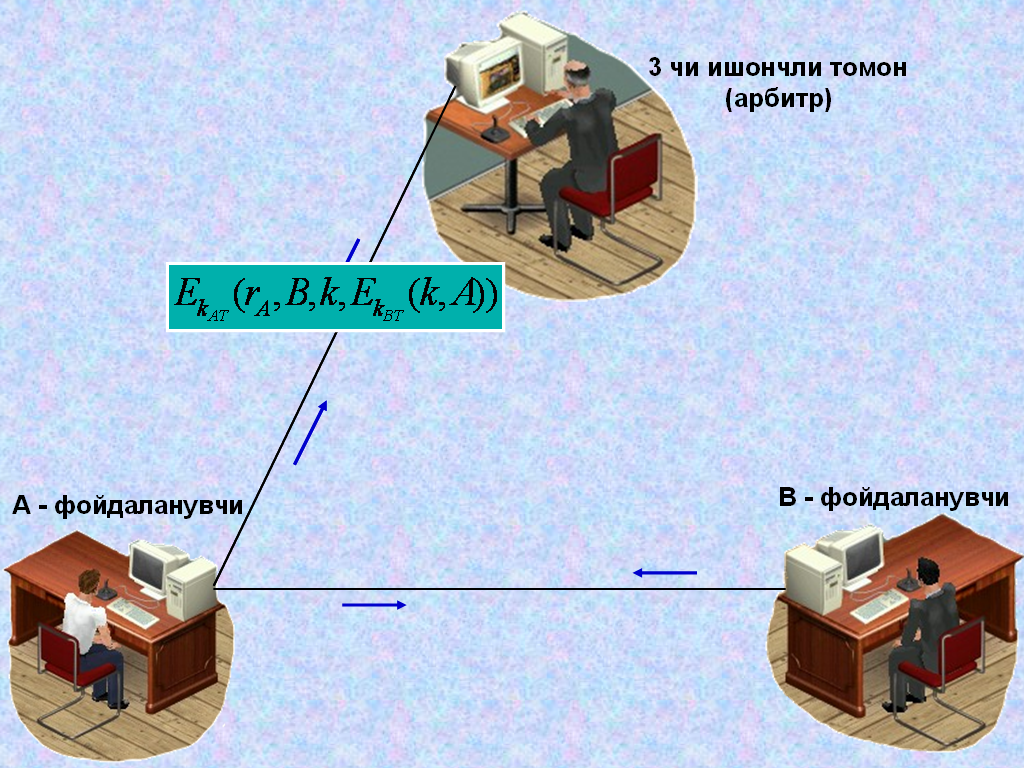
4. В - фойдаланувчи бу маълумотни дешифрлайди ва  - калитни олади. Сўнгра у тасодифий  - сонини генерация қилади. Бу тасодифий сонни -калит ёрдамида шифрлайди ва А -фойдаланувчига узатади:

В → А :  .

5. А - фойдаланувчи  - калит ёрдамида маълумотни дешифрлайди. А- фойдаланувчи тасодифий  - сонини генерация қилади. Бу сонни -калит ёрдамида шифрлаб қайта В -фойдаланувчига узатади:

A → В :  .

6. В - фойдаланувчи маълумотни дешифрлаб,  - сонини текширади ва ҳақиқатдан А - фойдаланувчи билан алоқа ўрнатаётганига ишонч ҳосил қилади.



Бу протоколда ,  ва  - сонларидан такроран фойдаланилади. Агар криптоаналитик аввал фойдаланилган  -калитни қўлга киритса, 3 - босқичда А -фойдаланувчи номидан В -фойдаланувчига маълумот узатиши мумкин.

**Криптоаналитик ҳужуми кетма-кетлиги**

1. Криптоаналитик В - фойдаланувчига қуйидаги маълумотни узатади:

С → В : .

2. В -фойдаланувчи  - калитни олади, тасодифиий  -сонини генерация қилади ва А - фойдаланувчига қуйидаги маълумотни узатади:

В → А: .

3. Криптоаналитик маълумотни қўлга киритиб,  -калит ёрдамида очади. У В *-*фойдаланувчига қуйидаги маълумотни узатади:

С → В:  .

4. В - фойдаланувчи маълумотни дешифрлаб ни олиб текширади. Сўнгра А -фойдаланувчи билан алоқа ўрнатаётганига ишонч ҳосил қилади.

Криптоаналитик В - фойдаланувчини шу тартибда ишонтириши мумкин.

**Хулоса.** Бу камчиликни бартараф этиш учун вақт белгисидан фойдаланиш мақсадга мувофиқ бўлади. Чунки 2) - босқичда ишончли томон маълумотига вақт белгиси қўшилади. Вақт белгиси тизимда аниқ ва ишончли вақтни талаб қилади.

Агар криптоаналитик А - фойдаланувчининг умумий калитини қўлга киритса, -сеанс калитга ҳам эга бўлиши ва Б - фойдаланувчи билан алоқа боғлаши мумкин. Бу ҳолат А - фойдаланувчи ўзининг умумий калитини ўзгартирган тақдирда ҳам давом этиши мумкин.

**Wide-Mouth Frog протоколи**

Ушбу протоколни ишончли сервер учун фойдаланиладиган калитларни алмашувчи симметрик протокол дейиш мумкин. А ва В - фойдаланувчилар арбитр билан биргаликда умумий калитлардан фойдаланадилар. Wide-Mouth Frogпротоколида А - фойдаланувчи В - фойдаланувчига сеанс калитни қуйидагича узатади:

1. А - фойдаланувчи вақт белгисини, В - фойдаланувчининг исмини ва сеанс калитни бирлаштириб умумий калит билан шифрлайди. Ўзининг исмини ва шифрматнни арбитр (W) га узатади:

А → W: .

2. Арбитр А - фойдаланувчининг малумотини дешифрлайди. Сўнгра янги вақт белгисини, А -фойдаланувчининг исмини ва сеанс калитни бирлаштириб ўзи ва В -фойдаланувчи учун умумий бўлган калит билан шифрлайди. Натижани В -фойдаланувчига узатади:

W → B: .

3. В - фойдаланувчи бу маълумотни қабул қилиб умумий калит билан дешифрлайди ва вақт белгисини олиб қабул қилган вақти билан солиштиради. Агар бу вақтлар орасидаги фарқ белгиланган интервалдан ошмаса  калитни ҳақиқий деб қабул қилади.

**Yahalom протоколи**

Бу пртоколга мувофиқ А ва В -фойдаланувчилар арбитр билан умумий калитдан фойдаланадилар. Протокол қадамлари кетма-кетлиги қуйидагидан иборат:

1. А - фойдаланувчи ўзи исми ва тасодифий сонини бирлаштириб, В- фойдаланувчига узатади:

A → B:  .

2. В - фойдаланувчи А - фойдаланувчининг исмини, унинг тасодифий сонини ва ўзининг тасодифий сонини бирлаштириб умумий калит билан шифрлайди. Ўзининг исмини ва натижани бирлаштириб арбитрга узатади:

B → W:  .

3. Арбитр иккита маълумотни ҳосил қилади. Биринчи маълумот В-фойдаланувчининг исми, сеанс калит, А ва В - фойдаланувчиларнинг тасодифий сонларидан ташкил топган. Бу маълумотни ўзининг ва А - фойдаланувчининг умумий калити билан шифрлайди. Иккинчи маълумот А -фойдаланувчининг исми ва сеанс калитидан ташкил топган. Арбитр бу маълумотни ўзи ва В - фойдаланувчи учун умумий бўлган калит билан шифрлайди. Сўнгра бу маълумотларни А -фойдаланувчига узатади:

W → A:  .

4. А - фойдаланувчи биринчи маълумотни дешифрлайди ва -калитни олади. У  ни 1)- босқичда узатилган қиймати билан солиштиради ва тўғри эканлигига ишонч ҳосил қилади. Сўнгра А -фойдаланувчи В- фойдаланувчига иккита маълумот узатади, биринчи – арбитрнинг маълумоти, иккинчиси – сеанс калит билан шифрланган  -тасодифий сон:

A → B: .

5. В - фойдаланувчи биринчи маълумотни дешифрлаб,  - калитни олади. Бу калит ёрдамида иккинчи маълумотни очиб, нинг қиймати 2) - босқичда юборилгани билан мос келишига ишонч ҳосил қилади.

Натижада А ва В - фойдаланувчилар айнан бир-бирлари билан алоқа боғлаганларига ишонч ҳосил қиладилар.

**Отвей-Риис протоколи**

Бу протоколда ҳам симметрик шифрлаш алгоритмидан фойдаланилади. Протокол қадамлари кетма-кетлиги қуйидагича:

1. А - фойдаланувчи тартиб рақами, ўзининг исми, В - фойдаланувчининг исми ва тасодифий  - сонидан ташкил топган маълумотни ҳосил қилади ва уни шифрлайди. Сўнгра у шифрматнни, тартиб рақамини, ўзининг ва В - фойдаланувчининг исмини В - фойдаланувчига узатади:

A → B: .

2. В -фойдаланувчи тасодифий -сони, тартиб рақами, А -фойдаланувчи ва ўзининг исмидан ташкил топган маълумотни ҳосил қилади. Бу маълумот умумий калит билан шифрланади. Сўнгра В -фойдаланувчи бу маълумотни, А -фойдаланувчи юборган маълумотни, тартиб рақами, ўзи ва А -фойдаланувчининг исмини арбитрга узатади:

B → W:  .

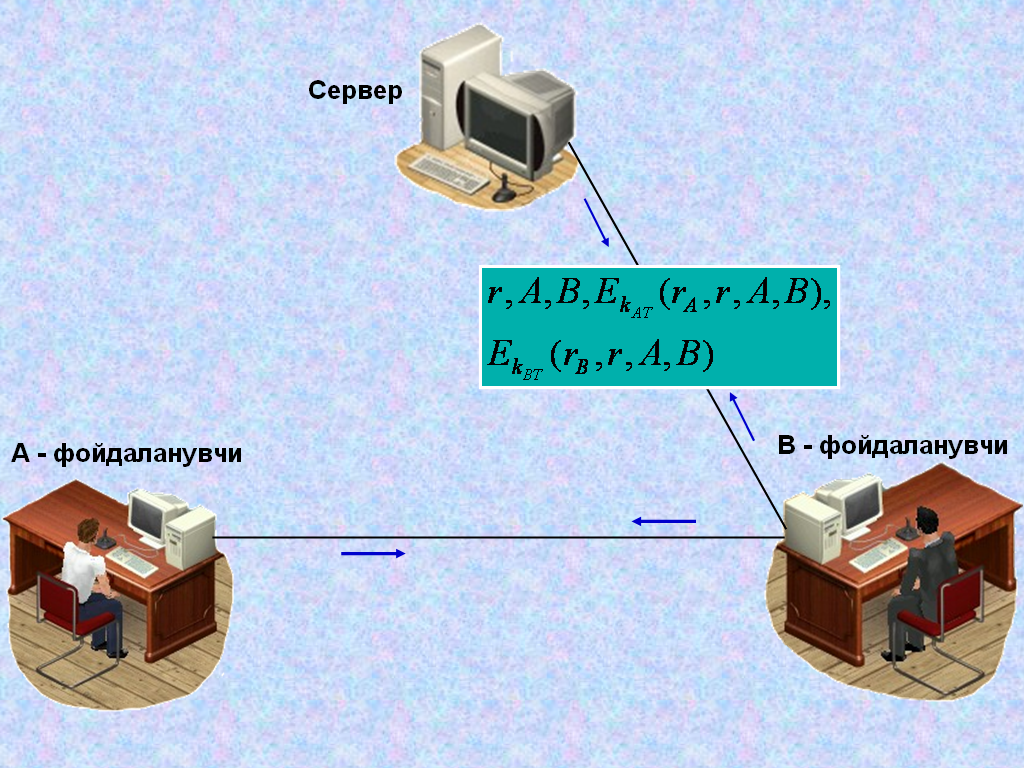
3. Арбитр тасодифий сеанс калитини хосил қилади. Сўнгра иккита маълумотни ҳосил қилади, биринчиси – А фойдаланувчининг умумий калити билан шифрланган А - фойдаланувчининг тасодифий - сони, иккинчиси – В фойдаланувчининг умумий калити билан шифрланган А- фойдаланувчининг тасодифий - сони. Арбитр тартиб рақамини ва иккала маълумотни бирлаштириб В -фойдаланувчига узатади:

W → B:  .

4. В - фойдаланувчи А - фойдаланувчининг калити билан шифрлаган тасодифий сон ва  -сеанс калитни А - фойдаланувчига узатади:

B → A:  .

5. А - фойдаланувчи маълумотни дешифрлаб ўзининг тасодифий сони ва - сеанс калитига эга бўлади. А - фойдаланувчи протокол бажарилиши натижасида улар ўзгармасдан қолганига ишонч ҳосил қилади .



Агар протокол бажарилиши натижасида барча тасодифий сонлар тўғри ва тартиб рақами ўзгармаган бўлса, у ҳолда А ва В - фойдаланувчилар бир-бирларининг хақ эканликларига ишонч ҳосил қиладилар ва ўзаро маълумот алмашиш учун маҳфий калитни қабул қиладилар.

***Neuman-Stubblebine* протоколи**

Тизимдаги бирор камчилик ёки соатлар синхронизациясининг носозлиги туфайли ишлатилмоқчи бўлаётган протокол амалга ошмаслиги мумкин. Агар узатувчининг соати қабул қилувчининг соатидан илгарилаб кетса, криптоаналитик узатувчининг маълумотини қабул қилиб, маълум вақтдан сўнг бу маълумотни такроран узатиши мумкин. “Яширин такрорий узатиш” деб номланган бу хужум усули кўнгилсиз оқибатларга олиб келиши мумкин.

Бу протокол яширин такрорий узатиш хужумига бардошли ҳисобланади. У Yahalom протоколининг яхшиланган варианти бўлиб, алгоритм қадамлари кетма-кетлиги қуйидагилардан иборат:

1. А фойдаланувчи ўзининг исмини ва тасодифий сонини В фойдаланувчига узатади:

А → В:  .

1. В фойдаланувчи бу маълумотга вақт, белгисини бирлаштириб, уни ўзи ва арбитр учун маълум бўлган калит билан шифрлайди. В фойдаланувчи ўзи исми, тасодифий сони ва шифрматнни арбитрга узатади:

В → W: .

1. Арбитр бу маълумотни олиб шифрматнни дешифрлайди. У сеанс калитни генерация қилади. Сўнгра у иккита маълумотни ҳосил қилади, биринчиси В - фойдаланувчининг исми, А - фойдаланувчининг тасодифий сони, сеанс калит ва вақт белгисидан иборат. Арбитр бу маълумотни ўзи ва А - фойдаланувчи учун умумий бўлган калит билан шифрлайди, иккинчи маълумот А - фойдаланувчининг исми, сеанс калит ва вақт белгисидан иборат. Арбитр бу маълумотни ўзи ва В - фойдаланувчи учун умумий бўлган калит билан шифрлайди. У иккала шифрматнни ва В - фойдаланувчининг тасодифий сонини А - фойдаланувчига узатади:

W → A:  .

1. А - фойдаланувчи биринчи шифрматнни дешифрлаб  -сеанс калитни олади ва  -тасодифий сонини 1) - босқичда юборилган қиймати билан тенг эканига ишонч ҳосил қилади. А -фойдаланувчи сеанс калит ёрдамида  -тасодифий сонни шифрлайди. У бу шифрматнни ва арбитрнинг иккинчи шифрматнини В -фойдаланувчига узатади:

А → В:  .

1. В -фойдаланувчи ўзининг калити ёрдамида биринчи шифрматнни очади ва  -сеанс калитга эга бўлади. Сеанс калит ёрдамида иккинчи шифрматнни очади ва тасодифий сонни ҳосил қилиб, 2) - чи босқичда узатилган қиймати билан тенг эканлигига ишонч ҳосил қилади.

Агар иккала тасодифий сонлар ва вақт белгилари мос бўлса, А ва В -фойдаланувчилар бир-бирларининг ҳақ эканлигига ишонч ҳосил қиладилар ва маҳфий калитни қабул қиладилар. Соатларнинг синхронизацияси талаб қилинмайди, вақт белгиси фақат В - фойдаланувчининг соати ёрдамида аниқланади ва фақат В - фойдаланувчигина вақт меткасини текшира олади.

Бу протоколнинг яна бир афзаллик томони шундан иборатки, А -фойдаланувчи арбитрдан қабул қилган малумотдан кейинчалик, В -фойдаланувчининг ҳақлигини текшириш учун бирор вақт оралиғида такроран фойдаланиши мумкин. Фараз қилайлик, А ва В -фойдаланувчилар юқорида келтирилган протоколни бажаришди ва сеанс алоқаси якунланди. Энди А ва В - фойдаланувчилар арбитрга мурожаат қилмасдан туриб бир-бирларининг ҳақ эканликларини текширишлари мумкин. Яъни:

1. А - фойдаланувчи учинчи босқичда арбитр томонидан юборилган шифрматнни ва янги тасодифий сонни В фойдаланувчига узатади:

А → В:  .

1. В - фойдаланувчи А - фойдаланувчининг тасодифий сонини сеанс калит билан шифрлайди. Бундан ташқари ўзи ҳам бошқа тасодифий сон ҳосил қилиб, шифрматн билан бирга А фойдаланувчига узатади:

В → А:  .

1. А -фойдаланувчи В -фойдаланувчининг тасодифий сонини сеанс калит билан шифрлаб В -фойдаланувчига узатади.

А → В:  . Янги тасодифий сонларни қайта узатиш натижасида пртоколнинг очилишини химоя қилиш мумкин экан.

2 )- босқичда узтилган тасодифий сонларнинг тўғри эканлигини текширади.

**Ньюман-Стабблайн протоколи**

1. А - фойдаланувчи ўз исми ва тасодифий сонини бирлаштириб, натижани Б - фойдаланувчига узатади:

A → В:  .

2) В - фойдаланувчи А - фойдаланувчининг исми, тасодифий сони ва вақт белгисини бирлаштириб умумий калит билан шифрлайди. Ўзининг исми ва тасодифий сонини натижага қўшиб, ишончли томонга узатади:

В → W: .

3) Ишончли томон тасодифий сеанс калитни генерация қилади ва иккита маълумотни ҳосил қилади, биринчиси – B - фойдаланувчининг исми, А - фойдаланувчининг тасодифий сони, сеанс калит ва вақт белгисидан иборат. Бу маълумотни умумий калит билан шифрлайди. Иккинчиси – А- фойдаланувчининг исми, сеанс калит ва вақт белгисидан ташкил топади. Бу маълумотни B - фойдаланувчининг умумий калити билан шифрлайди. Иккала шифрматнни ва B - фойдаланувчининг тасодифий сонини А- фойдаланувчига узатади:

W → А:  .

4) А - фойдаланувчи ишончли томоннинг умумий калити билан шифрланган маълумотни очиб  -калитни олади ва  нинг ҳақиқий эканига ишонч ҳосил қилади. А - фойдаланувчи B -фойдаланувчига иккита маълумот узатади. Биринчиси – B - фойдаланувчининг калити билан шифрланган арбитр маълумоти. Иккинчиси эса сеанс калит ёрдамида шифрланган  маълумот:

A → В:  .

5) В - фойдаланувчи бу маълумотни дешифрлайди ва  ни олади.  ва  ни 2 - босқичда юборилгани билан солиштиради ва маълумотнинг ҳақиқий эканига ишонч ҳосил қилади.

Агар иккита тасодифий сонлар ва вақт белгиси мос келса, А ва В -фойдаланувчилар сеанс калитни ўзаро ишлатаётганларига ишонч ҳосил қиладилар.

Шундан сўнг А ва В -фойдаланувчилар бир-бирларининг ҳақ эканликларини ишончли томоннинг иштирокисиз текширишлари мумкин.

1) А -фойдаланувчи 3 - босқичда ишончли томон унга юборган маълумотни ва янги тасодифий сонни В -фойдаланувчига узатади:

A → B:  .

2) В -фойдаланувчи А - фойдаланувчи юборган янги тасодифий сонни сеанс калит билан шифрлайди. У А - фойдаланувчига янги тасодифий сонни ва шифрматнни узатади:

В → А : .

3) А -фойдаланувчи В -фойдаланувчининг янги тасодифий сонини сеанс калит билан шифрлаб унга узатади:

A → В :  .

Ушбу ҳолат эса янги тасодифий сонлар такроран узатилиши мумкин бўлган хужумни бартараф этади.

**SKID протоколи**

SKID протоколи симметрик криптография асосида қурилган идентификация масаласини таъминлашга қаратилган бўлиб, унинг SKID2 ва SKID3 турлари мавжуд. Қуйида В -фойдаланувчига ўзининг ҳақлигини кўрсатиш имконини берувчи SKID2 протоколини кўриб чиқилади.

1) А - фойдаланувчи тасодифий  - сонини В -фойдаланувчига узатади.

2) В -фойдаланувчи тасодифий  - сонини олади. У  ни А- фойдаланувчига узатади. Бу ерда  – МАС код, В эса В -фойдаланувчининг исми.

3) А - фойдаланувчи  ни хисоблайди ва қабул қилгани билан солиштиради. Агар натижалар тенг бўлса, у ҳолда А - фойдаланувчи В -фойдаланувчи билан тўғри боғланганига ишонч ҳосил қилади.

**SKID3 протоколи** эса А ва В - фойдаланувчиларнинг тўлиқ аутентификациясини таъминлайди. 1, 3 - босқичлар SKID2 протоколи каби бажарилади:

4) А - фойдаланувчи НК(RВ, А) ни В - фойдаланувчига узатади. Бу ерда А, А - фойдаланувчининг исми.

5) B - фойдаланувчи  ни хисоблайди ва қабул қилгани билан солиштиради. Агар натижалар тенг бўлса, В -фойдаланувчи айнан А- фойдаланувчи билан боғланганига ишонч ҳосил қилади.

Ушбу протокол “Ўртадаги киши” хужумига бардошли эмас.

**Назорат саволлари**

1. Симметрик шифрлаш тизимлари асосида калитларни алмашиш.
2. Шамир протоколи.
3. Нидхам-Шрёдер протоколи.
4. Wide-Mouth Frog протоколи.
5. Yahalom протоколи
6. Отвей-Риис протоколи.
7. Neuman-Stubblebine протоколи
8. SKID протоколи.