AURREKO URTEETAKO AZTERKETA GALDERAK - SEGURTASUN BLOKEA

2013ko Maiatza

1. Galdera. Zein ala zeintzuk dira bai sinadura digitalaren bidez bai mezu autentifikazio kodeen (MAC kodeen) bidez eman daitezkeen segurtasun zerbitzuak? Eta zein ala zeintzuk dira teknika kriptografiko biak ezberdintzen dituzten segurtasun zerbitzuak? Erantzuna justifikatu.

Bai sinadura digitalak eta bai MAC kodeak funtzio berdina ematen dute: Mezu baten osotasuna edo jatorriarekiko autentifikazioa bermatzen dute, hau da, mezu horren jatorria ez dela dioenaren ezberdina. MAC kodeen eta sinadura digitalen arteko ezberdintasuna erabiltzen den kriptografia mota da. MAC-ek kriptografia simetrikoa erabiltzen du.

Mezua bera eta operazio matematiko baten (Hash bat, adibidez) emaitza batera ematen dira. Operazio matematikoak muturretako baten gakoarekin ere egiten da. Tarteko erasotzaile batek ez du gako hori izango, eta beraz, ezin izango du MAC kodea edo sinadura birsortu. Hartzaileak hau detektatuko du eta erreakzionatuko du.

2. Galdera. Zer da kriptoanalisia?

Sistemen ahultasunak aurkitzeko eta haien segurtasuna apurtzeko intentzioz sistema kriptografikoen azterketan datza kriptoanalisia. Kriptologiaren partea da. Azken finean, sistema batentzako erasoak planifikatzean datza.

1) Cyphertext-only erasoak: Erasotzaileak EZ daki ezer: dena enkriptatuta ikusten du
    1. Brute force
    2. Maiztasunen azterketan oinarritutakoa
    3. Kasiski metodoa
2) Known plaintext erasoak: Erasotzaileak testu arrunta ezagutzen du
    1. Ez da erasotzeko ezer geratzen, ezta…? EZ!
    2. Testu arruntaren parte bat ezagutzen badu soilik → “Probable word attack”
3) Chosen plaintext erasoak: Erasotzaileak nahi duen testua jarri dezake zifratzailetik
    1. Sortutako edozein testu zifratu eta aztertu dezake, beste noranzkoan egiteko bide baten bila
    2. Zifratzaile batek zifratutako edozein testu deszifratzeko gaitasuna lortzea da helburua honelako erasoetan.

3. Galdera. Zer da segurtasun politika bat? Zergatik da garrantzitsua? Zer nolako estrategiak erabili ohi dira segurtasun politikak definitzeko erakunde ezberdinetan?

Subjektuen eta objektuen artean baimendutako harremanak deskribatzen dituen dokumentu idatzi bat da. Garrantzitsua da prebentzio metodoak (Firewall, Antibirus, VPN, NAT…), detekzio metodoak (Intrusioak detektatzeko sistemak) baita erasoen aurreko erantzunak deskribatzen dituelako.

2013ko ekaina

4. Galdera. Demagun bi erabiltzaile dauzkagula eta bakoitzak bere ziurtagiri digitala daukala. Bi erabiltzaile hauek datuak trukatu nahi dituzte gako simetrikodun kriptografia erabiliz. Deskriba ezazu hau lortzeko burutu behar duten prozesua eta zehaztu erabili behar dituzten teknika kriptografikoak. Esplizituki adierazi kontutan hartutako suposizio guztiak.

Diffie-Hellman protokoloa erabiliz, gako simetriko bat lortu dezakete era seguroan. Erabiltzaileetako batek zenbaki lehen bat (p) eta sortzaile bat (g) aukeratu eta publikoki bidaliko dizkio beste erabiltzaileari. Edonork ezagutu ditzake arazorik gabe. Lehenengo Erabiltzaileak bere ziurtagiria (a) erabiliko du $A = g^a$ sortuz. A horren tamaina limitatzeko, p

zenbakiaren moduluarekin tamaina aldatuko zaio: $A = mod_p(g^a)$. Beste erabiltzaileak, bere ziurtagiria (b) erabiliko du bi gauza egiteko: $B = mod_p(g^b)$ sortzeko, lehen erabiltzaileari bidaliko diona, eta $K = mod_p(A^b)$ lortzeko. 1. erabiltzaileak K bera lor dezake: $K = mod_p(B^a)$

2013ko Uztaila

Galdera laburrak:
1. Galdera. Zein segurtasun zerbitzu ematen dira eta zeintzuk ez dira ematen mezu bat gako publiko batekin zifratzen denean? Erantzuna justifikatu.

Gako publiko batekin zifratzeak ez digu jatorriaren bermea ematen, gakoa bera publikoa denez, beste edonork ikusi eta erabili dezakeelako. Bai lortzen duguna, ordea, komunikazioaren konfidentzialtasuna da, enkriptaturiko informazioa delako azken finean.

2. Galdera. Zertarako balio du firewall batek? Zelan funtzionatzen du?

Erakunde baten barneko sarea Internet-etik isolatzen du, pakete batzuei pasatzen utziz eta beste batzuk blokeatuz. Hau router baten tokia hartu ohi du. Paketez pakete iragazten da trafikoa, eta honelako iragazkiak dira ohikoenak:

- Jatorri eta Helmuga IP-en arabera
- Jatorri eta Helmuga portuaren arabera
- ICMP mezu motaren arabera
- TCP-ren Three-Way Handshake-aren noranzkoa

3. Galdera. Zertan datza “brute force” edo “ciphertext only” deritzon eraso mota? Eta “known plain text” deritzona? Eta “chosen plain text” deritzona?

Brute force eraso baten ez dakigu deszifratzeko gakoa, beraz, gako posible guztiak, banan banan, frogatzen dira emaitzak ematen dituena lortu arte. Enkripzio mota oso kaskarretan bideragarria da honelako metodo hau.

Known plaintext eraso baten enkriptatutako mezuaren testu originalaren apur bat daukagu, eta beraz – enkripzio motaren arabera – antzeko hitzen bila edo bestelako patroien bilaketa errazten da.

Chosen plain text eraso baten, erasotzaileak enkripzio sisteman nahi duen informazioa sartu, enkrpitatu eta analizatu dezake, beraz, informazio asko lortzeko gaitasuna du, enkripzio motaren arabera.

4. Galdera. Zelan funtzionatzen du (zein da bere eginkizuna) eta zer ematen du KDC batek gako simetrikodun kriptografian? Laburki adierazi KDC batean erregistratutako bi erabiltzailek datuak trukatu nahi dituztenean eman beharreko pausuak.

KDC edo Key Distribution Centre batek gako bat partekatu nahi duten entitateen arteko sistema da. Sistema ezagun baten, 2 faseetako autentifikazioa ematen da:

- Autentifikazio fasea: Erabiltzaileak Ticket-ak lortzeko Ticket (TGT) bat lortzen du.
- TGT-aren bidez zerbitzuko Ticket bat lortzeko gaitasuna du erabiltzaileak, banakako zerbitzuek TGT-aren balidezia KDC-aren aurka konprobatuko dutelarik.
  Ticket-en eta TGT-aren erabilera-bizitza mugatuta dago.

2014ko Ekaina

1. Galdera. Azaldu nola sortzen den eta erabiltzaile batek zer behar duen sinadura digital egoki bat sortzeko. Adierazi sinadura digital batek zein segurtasun zerbitzu ematen dituen, erantzuna arrazoituz.

Bidali nahi den mezuaren hash-a gako pribatu batekin enkriptatu ostean lortzen dugu sinadura digitala. Sinadura hori mezuarekin batera bidaltzen denean, jatorria fidagarria dela jakin dezakegu: Sinadura-ren enkripzioa deseginez hash-a lortzen dugulako. Mezuaren hash-a birkalkulatu eta desenkriptatutakoa konparatuz. Berdinak badira, mezua dioen jatorritik etorri da.

2. Galdera. Kriptografia asimetrikoa darabilen sistema batean, zer da CA bat? Azaldu zein ataza burutu behar dituen.

CA Certification Authority edo Ziurtagiri Autoritatea da. Hauek fidagarriak dira, entitate finkoak direlako eta gure sistema eragileek zein nabigatzaileek dituzten ziurtagiriekin konprobatu daitezkeelako.

Hauen lana zera da: sinadura digital bat eta identitate bat lotu ahal izatea, adibidez, ehu-ko zerbitzariek emandako sinadurek eta ehu bera lotzeko.

2014ko Uztaila

1. Galdera. Zerbitzu hauek emateko, zein mekanismo erabiltzen dira?
   - Datuen jatorriaren autentikazioa
     MAC kodeak, sinadura digitalak.
   - Trafiko fluxuaren konfidentzialtasuna
     Enkripzioa, simetrikoa ala asimetrikoa.
   - Osotasuna
     MAC kodeak, sinadura digitalak.

2. Galdera. Zer da "mezuen freskotasuna"? Zein egoeratan erabiltzen da? Deskribatu ezagutzen dituzun freskotasun mekanismoak.

   Mezu baten freskotasuna mezu baten “adina” bezala ulertu daiteke. Freskotasuna garrantzitsua da errepikapen eraso baten aurka babesteko, zeinetan benetako mezu on bat geroago bidaltzen den. Mezu berbidali hori zaharkituta geratu dela detektatzean, eraso baten aurrean gaudela argi dago eta beraz informazioa ez diogu emango.

3. Galdera. A entitateak mezu luze bat bidali nahi dio B entitateari konfidentzialki, eta gainera, etorkizun batean mezu hori A entitateak berak sortu duela edozeini demostratu ahal izatea nahi du. Nola erabili dezake kriptografia hibridoa? Zein mekanismo erabili behar dira esandako zerbitzuak lortzeko?

   Mezu luze bat bidaltzeko gako simetrikodun kriptografia beharrezkoa da, kostu konputazionala dela eta. Gako simetrikoen lortzea ordea ere babestu beharra dago. Horretarako kriptografia hibridoa erabili daiteke. Lehenik hartzailearen giltza publikoarekin (asimetrikoa) gako simetrikoa zifratu eta bidaliko dugu:

   Hartzaileak haren gako pribatua erabiliz, gako simetrikoa lortuko du. Gako simetrikoa bi aldetan dugunean, mezu luzea horrekin enkriptatuko dugu eta bidali egingo dugu. Hartzaileak, gako simetrikoaren bidez desenkriptatuko du.

2015eko Maiatza

1. Galdera. MAC kodeak
   - Zer kriptografia mota erabiltzen dute MAC kodeek?
     MAC kodeek gako simetrikodun kriptografia mota erabiltzen dute.
   - Zertarako erabiltzen dira MAC kodeak? Adieraz ezazu zein edo zeintzuk diren MAC kodeek ematen dituzten segurtasun zerbitzuak, eta baita zein edo zeintzuk ez dituzten ematen, eta kasu bakoitza justifikatu.
     MAC kodeak edo Message Authentication Code-ak jatorriaren autentikazioa bermatzeko balio duten kodeak dira. Horrez gain, mezuaren osotasuna ere bermatzeko baliagarriak dira. Mezuaren jatorria dioena dela ziurtatzeko. Ez dute konfidentzialtasunik ezta mezuaren “adina” ematen.
   - Zer ezaugarri bete behar dituzte MAC kodeak kalkulatzeko erabiltzen diren algoritmoek?
     MAC algoritmoek gako simetriko bat eta mezu bat hartzen dituzte, eta luzeera finkoko balio bat ateratzen dute, MAC kodea bera. Gakoa ezagutu gabe mezu originala ezagutzea ezinezkoa

2. Galdera. Eraso pasiboak
   - Zer estrategia mota erabiltzen dira eraso pasiboen aurka babesteko?
     Eraso pasiboetan sistemak gainbegiratzean datza, konfidentzialtasunaren aurka egiteko asmoz.
   - Zeintzuk dira bereizten diren eraso pasibo mota ezberdinak?
     Informazioaren zabaltzea (desenkriptatzea) edo trafikoaren analisia (Zifratzea ezin daitekeenean desegin)
   - Eraso pasibo mota bakoitzak, zein segurtasun zerbitzutan dauka eragina?
     Konfidentzialtasuna mintzen duten erasoak dira.

- Zer mekanismo erabili daiteke eraso pasibo mota bakoitzaren aurrean babesteko?
  Enkripzio onaz baliatuz gelditu daitezke informazioaren zabaltzea medio duten erasoak. Bigarren motako erasoen lana zailagotzeko, trafiko faltsua sortu beharra dago, analisiaren emaitzak ezertarako balio ez dezaten.

3. Galdera. Kriptografia hibridoan, zertarako, zergatik eta nola erabiltzen da gako publikoko kriptografia?

Gako simetrikoa edo sesio gakoa babesteko erabiltzen da, sesioaren hasieran. Behin bi aldeek sesio gakoa (simetrikoa) dutela, mezu luzeak partekatu ditzakete horrekin.

2015eko Ekaina

1. Galdera. Osotasun segurtasun zerbitzua
   - Zertan datza osotasuna deritzon segurtasun zerbitzua?
     Baimenik gabeko aldaketen aurkako babesa ematen duen segurtasun zerbitzua da.
   - Zer mekanismo erabiltzen dira segurtasun zerbitzu hau bermatzeko?
     Sinadura digitalak eta MAC kodeak erabiltzen dira gehien bat.
   - Zertan datza mekanismo hauetariko bakoitza?
     Bien funtzionamendua antzekoa da: Mezuarekin batera zentzu bakarreko operazio baten emaitza ematen da. Operazio horrek bi sarrera hartzen ditu: Mezua bera eta mezua sortu duen erabiltzailearen informazio sekretua. Tarteko erasotzaile batek mezua aldatzekotan, ezin izango du sinadura edo kodea berreraiki.
2. Galdera. Eraso aktiboak
   - Zer estrategia mota erabiltzen dira eraso aktiboen aurka babesteko?
   - Zeintzuk dira bereizten diren eraso aktibo mota ezberdinak?
   - Eraso aktibo mota bakoitzak, zein segurtasun zerbitzutan dauka eragina?
3. Galdera. Ziurtagiri digitalak
   - Zein da ziurtagiri digitalen helburua?
   - Zeintzuk dira ziurtagiri digital baten ezinbesteko edukiak?
   - Segurtasun zerbitzuren bat inplementatzeko ziurtagiri digitalen erabilpena beharrezkoa den kasu baten adibidea ipini eta prozesua zelan burutuko zen azaldu.

2016ko Maiatza

1. Galdera. Zeintzuk dira gako sekretuko sistema kriptografikoen sendotasunean eragin gehien daukaten faktoreak? Eta gako publikoko sistema kriptografikoen sendotasunean? Zelan bermatu daiteke konfidentzialtasuna gako simetrikoko sistema bat erabiliz? Eta gako publikoko sistema bat erabiliz?

2. Galdera. Zeintzuk dira jatorriko autentikotasun eta ez ukatze segurtasun zerbitzuen artean existitzen diren ezberdintasunak? Zeintzuk dira zerbitzu hauetariko bakoitza inplementatzeko erabili daitezkeen mekanismoak eta zergatik?
3. Galdera. Justifika ezazu zer segurtasun zerbitzu eragiten den kasu bakoitzean
   a) Ekipo baten sistema eragilea erabiltezina bihurtzen da birus baten eraginez.
   b) Lapur batek datu pertsonalak gordeta dituen USB stick bat lapurtzen du.
   c) Hacker bat hari gabeko sare batean mezuak entzun, gorde eta beranduago birbidaltzeko gai da.

2016ko Ekaina

1. Galdera. Ziurtagiri digitalak
   a) Zein da ziurtagiri digitalen helburua?
      Gako publikoa bat eta haren jabearen arteko lotura autentifikatzea
   b) Zeintzuk dira ziurtagiri digital baten derrigorrezko edukiak?
      Gako publikoaren jabea, erlazioaren ziurtagiria eman duen autoritatea, balio epearen hasiera eta amaiera datak, serie zenbaki uniko bat.

c) Ipini behintzat 3 adibide zeinetan ziurtagiri digitalen erabilpena segurtasun zerbitzu bat ematea ahalbidetzen duen. Azaldu zelan lortzen den kasu bakoitzean.

1) Ziurtagiri digital batekin egiaztatu dezakegi Man Inin the long term The Middle eraso baten biktima ez garela izan. Horretarako, jasotako mezuetan erabiliko dugun gako publikoa ziurtagiritik lortutakoarekin konparatuz.

2)Ziurtagiri gurutzatuetaz baliatuz, beste ziurtagiri autoritate batek egindako ziurtagiri baten giltza lortu dezakegu.

2. Galdera. Sare baten trafikoaren behaketak, zer segurtasun zerbitzutan eragiten du? Azaldu zelan babestu gaitezkeen eraso mota honen aurrean.

Trafikoa konfidentziala ez bada, trafikoan zehar doan informazio guztia edonork lapurtu dezake. Era horretan edozein motatako jakituria eta eraso egin daitezke. Hau ekiditzeko, enkriptatu behar da.

Enkriptatutako trafikoa ordea ere badu nolabaiteko informazioa, zein zerbitzarietara/zerbitzarietatik datorren bereziki. Informazio hori izkutatzeko, gezurrezko trafikoa ere sortu beharra dago. Era horretan, trafikoa hausnartzen duen erasotzaile batek ez du informazio zehatzik izango trafikoaren noranzkoaren inguruan.

3. Galdera. Erabiltzen den kriptografia motaren arabera, zenbat gako trukatu behar dituzte, modu seguru batean, euren artean posta elektroniko zifratuak bidali nahi dituzten 5 pertsonatako talde batean? Zenbat gako dira beharrezkoak taldean 10 pertsona badaude? Zer gertatuko litzateke 10 izan beharrean 100 izango balira?

Partekatu behar diren gako kopurua esponentzialki igoko da, gero eta gehiagorekin partekatuy behar direlako. 5-ren kasuan 10 gako partekatu behar dira. 10-ren kasuan 45 gako eta 100-ren kasuan 4950 gako.

2017ko Maiatza

1. Galdera. Hurrengo kontzeptuak defini itzazu: segurtasun erasoa, segurtasun zerbitzua eta segurtasun mekanismoa. Hiru kontzeptu hauen arteko harremana azaldu.
2. Galdera. A erabiltzaile batek eduki publikoa daukan mezu bat bidali nahi dio B erabiltzaile bati, mezu honen osotasuna bermatuz. Zelan babestu behar du A erabiltzaileak bidalitako mezua, A eta B erabiltzaileek partekatutako gako sekretu bat badute? Eta erabiltzaile bakoitzak ziurtagiri digital bat badauka? Kasu bakoitzean jarraitutako prozesua deskriba ezazu.
3. Galdera. Zein da gako publikoen banaketan ziurtagiri digitalak erabiltzearen arrazoia?

2017ko Ekaina

1. Galdera. Zer segurtasun mekanismo ezagutzen dituzu hurrengo segurtasun zerbitzuak emateko: konfidentzialtasuna, ez ukatzea eta freskotasuna?
2. Galdera. Zer mekanismo ezagutzen dituzu MAC bat inplementatzeko?
3. Galdera. Zertan ezberdintzen dira nonce bat eta data zigilu bat?

2018ko Maiatza

1. Galdera. Azal ezazu zertan datzaten hurrengo erasoak eta zeintzuk diren euren arteko ezberdintasunak: ciphertext-only, known-plaintex, chosen-plaintext.
2. Galdera. Gako sekretudun eta gako publikodun kriptografien ezaugarriak konpara itzazu
3. Galdera. Demagun Alice erabiltzaileak mezu (M) konfidentzial eta autentifikatu bat bidali nahi diola Bob erabiltzaileari. Horretarako, Alice-ek ausazko gako simetriko bat sortzen du (KS) eta mezuaren hash-a kalkulatzen du (H(M)). Egoera honetan, zertarako erabiliko du Alice-ek bere gako pribatua? Eta Bob-en gako publikoa? Zehaztu ia komunikazio berean gako asimetriko bi hauen erabilpena bateragarria den. Zelan lortu dezakete Alice eta Bob-ek bestearen gako publikoa modu fidagarri batean?

2018ko Ekaina

1. Galdera. Zer da ziurtagiri digital bat? Zer erlazio dauka ziurtagiri-autoritateekin (CA-ekin)? Zertarako erabiltzen ditugu ziurtagiri digitalak Internet-en ibiltzen garenean?
2. Galdera. Zertan datza birbidaltze eraso bat? Zer motako erasoa da? Azaldu eraso hau ekiditeko erabili daitezkeen estrategia ezberdinak. Birbidaltze eraso batean, mezuaren osotasuna arriskuan jartzen da? Zergatik?

2019ko Maiatza

1. Galdera. Zelan sailkatzen dira kriptoanalisi erasoak? Mota bakoitza deskriba ezazu
2. Galdera. Gako sekretudun eta gako publikodun kriptografia konpara itzazu, honako alderdi hauek kontutan hartuz: bakoitzaren ezaugarriak, erabilitako gako kopurua eta segurtasunaren oinarria kasu bakoitzean.
3. Galdera. Zer informazio dauka ziurtagiri digital batek? Zein da nahitaezkoa? Ziurtagiria erabiltzen duen erabiltzaileak edo aplikazioak beste informazioren bat eduki behar du?

2019ko Uztaila

1. Galdera. Zer desberdintasun daude laburpen kriptografiko, MAC kode eta sinadura digital baten artean?
2. Galdera. Erdiko gizonaren erasoa (Man in the Middle Attack) deskriba ezazu. Zelan ekidin daiteke eraso hau?

2021eko Maiatza

1. Galdera. Zertan datza “ez ukatze” segurtasun zerbitzua? Zer mota existitzen dira? Deskribatu zerbitzu hau emateko erabiliko zenukeen mekanismoa edo mekanismoak, eta zelan erabiliko zenukeen edo zenituzkeen. Erantzuna lehen identifikatutako mota bakoitzarentzat zehaztu.
2. Galdera. Azaldu zergatik diren beharrezkoak ziurtagiri digitalak gako publikoko sistema kriptografikoetan. Zeintzuk dira ziurtagiri digitalek izan behar dituzten eremurik garrantzitsuenak? Ziurtagiri digitalak beharrezkoak al dira ere gako simetrikoko sistema kriptografikoen kasuan? Zure erantzuna justifikatu
3. Galdera. Algoritmo kriptografikoen gakoek bizitza erabilgarri bat daukate eta denbora hori pasatu ondoren, gomendagarria da gako hauek aldatzea. Ba al dago ezberdintasunen bat gako simetrikoko eta gako publikoko algoritmoen gakoen bizitza erabilgarriaren artean? Gako simetrikoko eta gako publikoko algoritmoen gakoen luzera bitetan adierazten da. Zergatik segurtasun maila berdintsua lortzeko, algoritmo mota batekin eta bestearekin erabili behar diren gakoen luzerak ez dira berdinak?

2021eko Ekaina

1. Galdera. Zer da zifratzaile sinple bat? Eta zifratzaile poligrafiko bat? Zer ezberdintasun daude zifratzaile monoalfabetiko eta polialfabetiko baten artean?

Zifratzaile sinple batek letrak banan banan zifratzen ditu. Poligrafiko batek, ordea, letra taldeak batera zifratzen ditu. Monoalfabetikoa eta polialfabetikoa orokorrean zifratzaile sinplearen barianteak dira. Batak ordezkatze berdina erabiltzen du mezu osoan zehar, eta besteak ordezkatzea aldatzen du mezuaren atal bakoitzean.

2. Galdera. A erabiltzaile batek B erabiltzaileak digitalki sinatutako dokumentu baten autentikotasuna egiaztatu nahi du. Horretarako, B-k bere ziurtagiri digitala bidaltzen dio A-ri, B-ren ziurtagiria CA2 ziurtagiri-autoritateak sinatu duelarik. Horretaz aparte, A-k badauka ere CA1 ziurtagiri-autoritatearen ziurtagiri digitala, baita ere CA1-ek CA2-rentzat sortutako ziurtagiri digital bat, CA1-ek sinatuta. A-k daukan informazioarekin, posiblea al da B-k sortutako sinadura digitalaren autentikotasuna egiaztatzea? Baiezko kasuan,

horretarako prozesua deskriba ezazu. Ezezko kasuan, azaldu zergatik eta zehaztu zer informazio falta den.

Posible izango da B-ren ziurtagiria konprobatzea, A erabiltzaileak CA-en ziurtagiri gurutzatuak dituelako. CA1-ren giltzapublikoa erabiliz, CA2-ren giltza publikoa lor daiteke. CA2-ren giltza publikoa erabiliz, B-ren giltza publikoa lor daiteke, era horretan B-ren identitatea ziurtatuz.

3. Galdera. A erabiltzaile batek gako sekretu bat konpartitu nahi du B erabiltzaile batekin, Diffie Hellman-en bidez. Zertan datza erdiko gizonaren ("Man-In-The-Middle") erasoa? Kasu honetan eraso hori gertatu daiteke? Baiezko kasuan, erasoa grafikoki deskribatu. Ezezko kasuan azaldu zergatik.

Posible da Diffie-Hellman metodoaren erdian Man-In-The-Middle eraso bat gertatzea, ez badira bidaltzen diren mezuak sinatzen edo MAC kode batekin markatzen: Mezu hauek beraien kabuz ez dute autentifikazio mekanismorik.

Tarteko erasotzaile batek A erabiltzaileak bidalitako g^a harrapatu dezake, bere g^c rekin erantzun eta era horretan giltz bat partekatuko du A-rekin, B erabiltzailea konturatu gabe. Horren ostean, C erasotzailea B-rekinjarriko da harremanetan, oraingoan A-ren posizioa hartuz.

2022ko Maiatza

1. Galdera. Adibide zehatz bat erabiliz, azaldu zelan erabili daitezkeen ziurtagiri digitalak erdiko gizonaren erasoa ekiditeko

2. Galdera. Zelan sailkatzen dira kriptoanalisi erasoak, erasotzailearen ezagutzaren arabera? Mota bakoitza deskriba ezazu

1. Cyphertext-only erasoak: Erasotzaileak EZ daki ezer: dena enkriptatuta ikusten du
   - Brute force
   - Maiztasunen azterketan oinarritutakoa
   - Kasiski metodoa
2. Known plaintext erasoak: Erasotzaileak testu arrunta ezagutzen du
   - Ez da erasotzeko ezer geratzen, ezta…? EZ!
   - Testu arruntaren parte bat ezagutzen badu soilik → "Probable word attack"
3. Chosen plaintext erasoak: Erasotzaileak nahi duen testua jarri dezake zifratzailetik
   - Sortutako edozein testu zifratu eta aztertu dezake, beste noranzkoan egiteko bide baten bila

Zifratzaile batek zifratutako edozein testu deszifratzeko gaitasuna lortzea da helburua honelako erasoetan.

3. Galdera. Hurrengo segurtasun zerbitzuak deskriba itzazu: osotasuna, autentikotasuna eta ez ukatzea. Zerbitzu bakoitza inplementatzeko erabili daitezkeen teknikak azaldu, haien arteko ezberdintasunak nabarmenduz.

Osotasuna: Mezu bat jatorritik irten denetik helmugara heldu den arte aldaketa ez baimendurik jasan ez duela zirutatzean datza.

Autentikotasuna: Mezuaren jatorria mezuak dioena dela eta ez erasotzaile baten ekskuetatik datorren mezua izatea.

Ez ukatzea: Zerrbitzu bat martxan jarraitzea benetako erabiltzaileentzat zerbitzatzen.

2022ko Ekaina

1. Galdera. Konpara itzazu freskotasuna emateko erabiltzen diren 3 mekanismo hauek: (1) data zigiluak (timestamp), (2) data zigilu logikoak (sekuentzia zenbakiak) eta (3) nonce-ak. 3 mekanismoak konparatzerako orduan, ondorengo alderdi hauek har itzazu kontuan: sinkronizazio beharrak, egoera informazioa biltegiratzeko beharra eta bidali beharreko mezu kopurua.

Data zigilu arruntak izatean, bi muturren erlojuak sinkronizatuta egon behar dira. Sekuentzia zenbakiak erabiltzean, ez da denbora kontutan hartzen, ordena baizik. Horregaitik sekuentzia zenbakiak errepikatzeko errazagoak dira.

Nonce-ak erabiltzean ekiditzen da, zerbitzariak zenbaki aleatorio bat sortzen duelako, baina mezu truke gehiago daude (3, challenge-etan) eta beraz ez dira oso eraginkorra.

2. Galdera. Deskriba eta konpara itzazu kriptografia simetrikoan eta asimetrikoan, gakoen banaketarako erabiltzen diren mekanismoak. Kriptografia simetrikoaren kasuan, A eta B entitate bi, haien artean modu seguru baten komunikatu nahi badira, aldez aurretik gakoen banaketarako zerbitzariarekin komunikatu behar dira beti? Zure erantzuna justifikatu

2023ko Maiatza

1. Galdera. Eraso motak deskriba itzazu grafikoak erabiliz.
2. Galdera. Gaurko segurtasun sistemetan, nola konbinatzen dira kriptografia simetrikoa eta asimetrikoa? Zergatik egiten da horrela? Sinatze edo zifratze kasua deskriba ezazu.
3. Galdera. Vigenére zifratze adibide hau deszifra ezazu atxikitako taula erabiliz. Azaldu zergatik hizki berdina hiru era desberdinetan deskodetzen den. Erantzun horretan oinarrituz, algoritmo hau, nola sailkatuko zenuke?

k= CRYPTO
c= YYYITBKTCSTMVFBPR
¿m?
WHATANICEDAY

Tablero de Vigenère

0	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	**U**	**V**	**W**	**X**	**Y**	**Z**	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	**Z**	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**

2023ko Ekaina

1. Galdera. Erasotzailearen aurretiko ezagutzaren araberako kriptoanalisi eraso motak deskriba itzazu.

4. Cyphertext-only erasoak: Erasotzaileak EZ daki ezer: dena enkriptatuta ikusten du
   - Brute force
   - Maiztasunen azterketan oinarritutakoa
   - Kasiski metodoa
5. Known plaintext erasoak: Erasotzaileak testu arrunta ezagutzen du
   - Ez da erasotzeko ezer geratzen, ezta…? EZ!
   - Testu arruntaren parte bat ezagutzen badu soilik → "Probable word attack"
6. Chosen plaintext erasoak: Erasotzaileak nahi duen testua jarri dezake zifratzailetik
   - Sortutako edozein testu zifratu eta aztertu dezake, beste noranzkoan egiteko bide baten bila
   - Zifratzaile batek zifratutako edozein testu deszifratzeko gaitasuna lortzea da helburua honelako erasoetan.

2. Galdera. Adibide konkretu bat erabiliz, azal ezazu nola erabil daitezkeen ziurtagiri digitalak erdiko gizonaren erasoa (Man in the Middle Attack) ekiditeko.

Ziurtagiri digitalek Ziurtagiri Autoritate fidagarrien "sinadura" dute. Hauen bidez, gako publiko bat identitate bati lotzen da. Demagun Alice-ri mezu bat bidali nahi diogula era konfidentzialean, horretarako, haren giltz publikoa behar izango dugu. Giltza berea dela ziurtatzeko Alice-ri haren ziurtagiria eskatuko diogu. Ziurtagiri hori sinatu duen Ziurtagiri Autoritatearen giltz publikoarekin desenkriptatuz, Alice-ren gako publikoa lor dezakegu eta ziur egon gaitezke lortutako gakoa ez dela beste edonorrena.