Distribucija ključa

Berghaus, Inga

Sveučilište J. J. Strossmayera u Osijeku
Odjel za matematiku
Diplomski studij Financijska matematika i statistika

Inga Berghaus

Distribucija ključa

Diplomski rad

Osijek, 2016.

Sveučilište J. J. Strossmayera u Osijeku
Odjel za matematiku
Diplomski studij Financijska matematika i statistika

Inga Berghaus

Distribucija ključa

Diplomski rad

Mentor: izv. prof. dr. sc. Ivan Matić

Osijek, 2016.

Sadržaj

1. Uvod

Kriptografija je znanstvena disciplina koja se bavi proučavanjem metoda za slanje poruka u takvom obliku da ih samo onaj kome su namijenjene može pročitati. Dvije strane (pošiljatelj i primatelj) komuniciraju preko nesigurnog komunikacijskog kanala (internet, telefonska linija), te pritom postoji mogućnost da treća strana (njihov protivnik), koja može nadzirati komunikacijski kanal, otkrije sadržaj poruke. Poruka koju pošiljatelj šalje primatelju zove se otvoreni tekst, a pošiljatelj ga šifrira koristeći unaprijed dogovoreni ključ. Dobiveni tekst zove se šifrat. Primatelj uz pomoć ključa može dešifrirati šifrat i pročitati otvoreni tekst.

Ključ može biti javni ili tajni, pa tako razlikujemo kriptografiju tajnog ključa i kriptografiju javnog ključa. U kriptografiji tajnog ključa pošiljatelj i primatelj odabiru tajni ključ koji generira funkcije za šifriranje i dešfriranje. Prije šifriranja poruke, pošiljatelj i primatelj moraju razmijeniti tajni ključ preko sigurnog komunikacijskog kanala. Ovo je i glavni nedostatak kriptografije tajnog ključa, jer se ključevi moraju često mijenjati, a i ukoliko postoji siguran komunikacijski kanal, preko njega bi se poruke mogle prenositi direktno, bez šifriranja. Kod kriptografije javnog ključa, funkcija šifriranja je javno dostupna, ali se funkcija dešifriranja ne može otkriti u nekom razumnom vremenu. Proces slanja poruke funkcionira tako da primatelj poruke prvo pošalje svoj javni ključ pošiljatelju poruke. Pošiljatelj šifrira svoju poruku pomoću dobivenog ključa i šifrat šalje primatelju. Primatelj dešifrira šifrat koristeći svoj tajni ključ. Ako više strana želi komunicirati na ovaj način, tada svi stavljaju svoje javne ključeve u javnu, svima dostupnu datoteku. Primatelj ne šalje svoj javni ključ pošiljatelju, nego ga pošiljatelj jednostavno pročita iz datoteke.

Glavne prednosti korištenja kriptografije javnog ključa su te što nema potrebe za sigurnim komunikacijskim kanalom za razmjenu ključeva, a za komunikaciju grupe od n strana potrebno je $2n$ ključeva, za razliku od $\binom{n}{2}$ ključeva kod kriptografije tajnog ključa. Kriptosustavi s javnim ključem su mnogo sporiji, pa se za dešifiranje dugih poruka koriste kriptosustavi s tajnim ključem. U realnom svijetu, koristi se kombinacija kriptografije tajnog i javnog ključa. Kriptografija javnog ključa se koristi za šifriranje ključeva, a kriptografija tajnog ključa za šifriranje poruka.

U radu će biti opisane sheme distribucije ključa i analizirana sigurnost pojedinih shema.

2. Distribucija ključa

Pretpostavimo da imamo nesigurnu mrežu sa n korisnika. Neke sheme uključuju povjerljivi autoritet koji je odgovoran za provjeru identiteta korisnika, izdavanje certifikata i odabir i prenošenje ključa do korisnika.

S obzirom na vrijeme trajanja ključa, razlikujemo dugotrajne ključeve i ključeve određenog razdoblja.

Dugotrajni ključevi se kreiraju, sigurno pohranjuju i koriste kada je to potrebno. Određuju se na temelju tajnih informacija, a mogu biti javni i tajni. Tajni dugotrajni ključevi poznati su samo paru korisnika ili jednom korisniku i povjerljivom autoritetu. Javni dugotrajni ključevi su usklađeni s tajnim ključevima koji su pohranjeni na certifikatima korisnika. Dugotrajni ključevi se najčešće koriste u protokolima za prijenos šifriranih ključeva određenog razdoblja ili za identifikaciju podataka.

Ključevi određenog razdoblja vrijede kratko vremensko razdoblje, te se odbacuju nakon što to razdoblje završi. Najčešće su tajni i koriste se u kriptosustavima s tajnim ključem. Postoji nekoliko razloga zašto su ključevi određenog razdoblja korisni. Ograničavaju količinu šifriranog teksta dostupnog napadaču, jer se ključevi određenog razdoblja redovito mijenjaju. Također, ograničavaju izloženost u slučaju otkrivanja ključa određenog razdoblja (poželjno je da se ne otkriju dugotrajni ključevi ili drugi ključevi određenog razdoblja). I na kraju, korištenje ključa određenog razdoblja smanjuje količinu dugoročnih informacija koje se moraju sigurno pohraniti kod svakog korisnika, jer se ključevi za parove korisnika generiraju samo kada je to potrebno. Zbog navedenih razloga, ključevi određenog razdoblja se mogu koristiti u rizičnim okruženjima gdje je mogućnost napada vrlo velika.

Postoje tri pristupa problemu uspostave javnog ključa, odnosno tri sheme distribucije ključa.

Shema predistribucije ključa

Povjerljivi autoritet prenosi informaciju o ključu u sigurnom obliku prije vremena distribucije ključa svim korisnicima na mreži. Informacija o ključu je potrebna kako bi se generirao tajni ključ. Svi korisnici koriste tajne ključeve za šifriranje poruka koje šalju preko mreže. Svaki par korisnika na mreži na temelju informacije o ključu može odrediti ključ poznat samo njima. Nakon što korisnici kreiraju svoje tajne ključeve, mogu se kreirati ključevi određenog razdoblja, pomoću npr. sheme dogovora ključa. Glavni problem kod sheme predistribucije ključa je količina tajnih informacija koje svaki korisnik na mreži mora pohraniti. Odgovarajuća shema predistribucije ključa može značajno smanjiti zahtjev za velikom količinom prostora za pohranu.

Shema distribucije ključa određenog razdoblja

Povjerljivi autoritet odabire ključeve određenog razdoblja i šalje ih korisnicima kada oni to zatraže. Šifriraju se koristeći prethodno kreirane tajne ključeve (pod pretpostavkom da svaki korisnik posjeduje tajni ključ čija vrijednost je poznata povjerljivom autoritetu). Korisnici zahtjevaju male količine prostora za pohranu, dok povjerljivi autoritet zahtjeva vrlo velike količine prostora za pohranu podataka.

Shema dogovora ključa

Shema dogovora ključa označava protokol u kojem dvije ili više strana zajedno kreiraju tajni ključ međusobno komunicirajući preko javnog kanala. Ključ se ne transportira od jedne do druge strane kao što je to slučaj kod sheme distribucije ključa određenog razdoblja. Shema dogovora ključa može koristiti i tajni i javni ključ. U shemi dogovora ključa povjerljivi autoritet nema aktivnu ulogu, a ponekad se i ne koristi. Ako se shema dogovora ključa temelji na javnom ključu, tada je povjerljivi autoritet potreban za izdavanje certifikata i za održavanje infrastrukture javnog ključa. Kod sheme s tajnim ključem, povjerljivi autoritet ranije distribuira ključ i tada svaki par korisnika ima tajni dugotrajni ključ poznat samo njima. U 'naivnoj' implementaciji svaki korisnik pohranjuje $n - 1$ dugotrajnih ključeva, što zahtjeva veliku količinu prostora za pohranu, ako je n velik. Shema dogovora ključa s javnim ključem traži da svi korisnici imaju svoj par javnih/privatnih dugotrajnih ključeva. To zahtjeva malo prostora za pohranu, jer korisnici sami pohranjuju svoj tajni ključ i certifikat s javnim ključem.

Zaštita od napadača

Osim pošiljatelja i primatelja, na mreži se često nalazi i treća strana ili više njih koji žele saznati sadržaj poruke iako njima nije namijenjena. Možemo je zvati protivnik, napadač ili imenom, Oscar. Zaštita od napadača je vrlo važna, jer kriptiranje poruke nema smisla ako je može pročitati bilo tko.

Pretpostavimo da je napadač Oscar jedan od korisnika na mreži. Kao napadač, on može biti aktivan ili pasivan. Kao pasivni napadač, može samo čitati poruke koje se prenose kanalima. Kao aktivni napadač, on može učiniti sljedeće: promijeniti poruke, sačuvati poruke pa ih kasnije koristiti, ili se lažno predstaviti kao neki drugi korisnik na mreži. Ciljevi napada mogu biti:

1. Podmetnuti nevaljan ključ - npr. stari ključ kojem je isteklo vrijeme trajanja.
2. Uvjeriti korisnike U i V da su razmjenili ključeve, iako to oni nisu učinili.
3. Otkriti neke informacije o ključu koji su razmijenili korisnici U i V.

Prva dva cilja zahtjevaju aktivni napad, dok se treći cilj može ostvariti i pasivnim napadom. Postoje različiti modeli napada, na primjer, napad kod kojeg je protivniku poznat ključ određenog razdoblja, ali je cilj zaštititi preostale ključeve. Posebno je opasan napad na dugotrajne ključeve kod kojeg su napadaču poznati dugotrajni ključevi svih sudionika. Koliko su pojedine sheme sigurne od napadača, biti će navedeno kod svake koja će biti obrađena, ali kod sheme distribucije ključa određenog razdoblja i sheme dogovora ključa poželjno je da napadač ne može saznati vijednosti ključeva određenog razdoblja iz prethodnih razdoblja. Cilj sheme distribucije ključa određenog razdoblja i sheme dogovora ključa je da na kraju određenog razdoblja korisnici U i V posjeduju isti ključ K čija vrijednost je poznata samo njima (osim eventualno i povjerljivom autoritetu).

3. Diffie - Hellmanova predistribucija ključa

Diffie - Hellmanova predistribucija ključa omogućuje da dvije strane kreiraju tajne ključeve razmjenjujući poruke preko otvorenog kanala.

Pretpostavimo da je $(G, \cdot)$ grupa i neka je α element grupe G reda n, tj. $\alpha^n = e$, neutralnom elementu grupe G i $\alpha^m \neq e$, za $1 \leq m < n$. Svaki korisnik U ima privatni dugotrajni ključ a_U (gdje je $0 \leq a_U \leq n-1$) i odgovarajući javni ključ $b_U = \alpha^{a_U}$. Analogno, svaki korisnik V ima privatni dugotrajni ključ a_V (gdje je $0 \leq a_V \leq n-1$) i odgovarajući javni ključ $b_V = \alpha^{a_V}$. Korisnički javni ključevi pohranjeni su na certifikatima, a potpisuje ih povjerljivi autoritet. Dugotrajni ključ za bilo koja dva korisnika U i V, definira se kao $K_{U,V} = \alpha^{a_U a_V}$.

Algoritam 1. Diffie - Hellmanova predistribucija ključa

1. Javni parametri sadržani su u grupi $(G, \cdot)$ i element $\alpha \in G$ je reda n.
2. Korisnik V određuje $K_{U,V} = \alpha^{a_U a_V} = b_U^{a_V}$, koristeći javni ključ b_U iz certifikata korisnika U i svoj privatni ključ a_V.
3. Korisnik U određuje $K_{U,V} = \alpha^{a_U a_V} = b_V^{a_U}$, koristeći javni ključ b_V iz certifikata korisnika V i svoj privatni ključ a_U.

Primjer 1. Pretpostavimo da su $p = 12987461$, $q = 1291$ i $\alpha = 3606738$ parametri javne domene. Brojevi p i q su prosti,

$$p - 1 \equiv 0 \pmod{q},$$

i α je reda q. Primijenjujemo Algoritam 1. na podgrupu $(\mathbb{Z}_p^*, \cdot)$ reda q. Pretpostavimo da U bira $a_U = 357$. Tada on računa:

$$\begin{aligned} b_U &= \alpha^{a_U} \mod p \\ &= 3606738^{357} \mod 12987461 \\ &= 7317197, \end{aligned}$$

koji se nalazi na njegovom certifikatu. Pretpostavimo da V bira $a_V = 199$. Tada on računa:

$$\begin{aligned} b_V &= \alpha^{a_V} \mod p \\ &= 3606738^{199} \mod 12987461 \\ &= 138432, \end{aligned}$$

koji se nalazi na njegovom certifikatu. Sada U može odrediti ključ

$$\begin{aligned} K_{U,V} &= b_V^{a_U} \mod p \\ &= 138432^{357} \mod 12987461 \\ &= 11829605, \end{aligned}$$

i V može odrediti isti ključ

$$\begin{aligned} K_{U,V} &= b_U^{a_V} \mod p \\ &= 7317197^{199} \mod 12987461 \\ &= 11829605. \end{aligned}$$

Koliko je ova shema sigurna u slučaju napada? Diffie - Hellmanova predistribucija ključa je sigurna samo u slučaju pasivnih napada i niti jedna strana ne zna je li poruka ili druga strana autentična. Pod pretpostavkom da su korisnički privatni ključevi sigurni, ne treba uzeti u obzir mogućnost aktivnog napada. Možemo se jedino pitati da li napadač (npr. W) može izračunati $K_{U,V}$, ako je $W \neq U, V$. Problem sigurnosti svodi se na to da li protivnik može izračunati tajni ključ $K_{U,V} = \alpha^{a_U a_V}$, poznavajući javne ključeve α^{a_U} i α^{a_V}.

Ako i napadač ne može otkriti Diffie - Hellmanov ključ, postoji mogućnost da otkrije djelomične informacije o ključu. Zato je cilj semantička sigurnost ključeva, što znači da napadač ne može otkriti niti djelomične informacije o ključu. Razlikovanje Diffie - Hellmanovih ključeva od slučajnih elemenata podgrupe $\langle\alpha\rangle$ treba biti onemogućeno. Ovdje je s $\langle\alpha\rangle$ označena ciklička grupa generirana s α.

Shema se smatra sigurnom za pravi izbor javnih parametara i grupe. Jedna je od rijetkih shema koja i unatoč otkrivanju dugotrajnog ključa onemogućava otkrivanje ključeva određenog razdoblja koji su generirani prije otkrivanja dugotrajnog ključa.

4. Bezuvjetno sigurna predistribucija ključa

U nastavku je opisan trivijalan slučaj bezuvjetno sigurne predistribucije ključa. Za svaki par korisnika U i V, povjerljivi autoritet bira slučajan ključ $K_{U,V} = K_{V,U}$, i šalje ga korisnicima U i V preko sigurnog kanala (mreža nije sigurna pa se prijenos ključa ne odvija preko mreže). Svaki korisnik mora pohraniti $n-1$ ključ i povjerljivi autoritet teba sigurno poslati ukupno $\binom{n}{2}$ ključeva. Ovaj slučaj je teško provediv u praksi jer je preskup i za relativno male mreže. Cilj je smanjiti količinu informacija koje se trebaju prenijeti i pohraniti, ali omogućujući pritom da svaki par korisnika može izračunati tajni ključ $K_{U,V}$. Ovaj slučaj opisuje Bloomova shema predistribucije ključa.

4.1. Bloomova shema predistribucije ključa

Pretpostavimo da povjerljivi autoritet sigurno distribuira tajne informacije korisnicima na mreži (njih n). Shemu može napasti podskup od najviše k protivnika i otkriti tajne informacije korisnika, pri čemu je k prije određen sigurnosni parametar. Cilj protivnika je otkriti tajni dugotrajni ključ para korisnika. Bloomova shema predistribucije ključa je shema predistribucije ključa koji je bezuvjetno sigurna od napada takvog tipa. Uvjet sigurnosti je sljedeći: Svaki skup od najviše k protivnika (različit od U, V) ne smije biti u mogućnosti odrediti bilo koju informaciju o $K_{U,V}$.

U Bloomovoj shemi predistribucije ključa, ključevi se biraju iz konačnog polja $\mathbb{Z}_p$, $p \geq n$, p je prost. Sa $\mathbb{Z}_p$ je označen skup svih ostataka modulo p. Povjerljivi autoritet će poslati $k+1$ elemenata iz $\mathbb{Z}_p$ svakom korisniku preko sigurnog kanala (u odnosu na $n-1$ element u trivijalnoj shemi predistribucije ključa). Količina informacija koju prenosi povjerljivi autoritet je neovisna o n.

Sljedeći alogritam opisuje posebni slučaj Bloomove sheme predistribucije ključa, u kojem je $n = 1$. Povjerljivi autoritet će poslati dva elementa iz $\mathbb{Z}_p$ svakom korisniku preko sigurnog kanala. Nitko drugi neće moći odrediti niti jednu informaciju o $K_{U,V}$.

Algoritam 2. Bloomova shema predistribucije ključa, $n = 1$

1. Prost broj p je javan, i za svakog korisnika U, element $r_U \in \mathbb{Z}_p$ je javan. Elementi r_U moraju biti različiti.

2. Povjerljivi autoritet odabire tri različita elementa $a, b, c \in \mathbb{Z}_p$ i kreira polinomijalnu funkciju

$$f(x, y) = a + b(x + y) + cxy \mod p.$$

3. Za svakog korisnika U, povjerljivi autoritet računa polinomijalnu funkciju

$$g_U(x) = f(x, r_U) \mod p$$

i šalje $g_U(x)$ prema U preko sigurnog kanala. Funkcija $g_U(x)$ je polinomijalna u x, pa možemo pisati

$$g_U(x) = a_U + b_U x,$$

gdje je

$$a_U = a + br_U \mod p$$

i

$$b_U = b + cr_U \mod p.$$

4. Ako U i V žele komunicirati, tada upotrebljavaju ključ

$$K_{U,V} = K_{V,U} = f(r_U, r_V) = a + b(r_U + r_V) + cr_U r_V \mod p,$$

gdje U određuje ključ

$$K_{U,V} = g_U(r_V)$$

i V određuje ključ

$$K_{V,U} = g_V(r_U).$$

Napomena 1. Polinomijalna funkcija f je simetrična: $f(x, y) = f(y, x)$, za sve x, y. Ovo svojstvo osigurava da vrijedi $g_U(r_V) = g_V(r_U)$, pa tako U i V kreiraju isti ključ u četvrtom koraku algoritma.

Bloomova shema predistribucije ključa za $n = 1$, opisana je u sljedećim primjeru.

Primjer 2. Pretpostavimo da imamo tri strane U, V i W, $p = 17$, i parametri javne domene su $r_U = 12$, $r_V = 7$ i $r_W = 1$. Pretpostavimo da povjerljivi autoritet odabire $a = 8$, $b = 7$ i $c = 2$, tako da je polinomijalna funkcija f oblika

$$f(x, y) = 8 + 7(x + y) + 2xy.$$

Polinomijalne funkcije g su oblika kako slijedi:

$$g_U(x) = 7 + 14x,$$

$$g_V(x) = 6 + 4x,$$

$$g_W(x) = 15 + 9x.$$

Ključevi su redom

$$K_{U,V} = 3,$$

$$K_{U,W} = 4,$$

$$K_{V,W} = 10.$$

Korisnik U određuje ključ

$$K_{U,V} = g_U(r_V) = 7 + 14 \cdot 7 \mod 17 = 3,$$

dok korisnik V određuje ključ

$$K_{V,U} = g_V(r_U) = 6 + 4 \cdot 12 \mod 17 = 3.$$

Slijedi dokaz da niti jedan korisnik ne može otkriti ključ druga dva korisnika.

Teorem 1. Bloomova shema predistribucije ključa za $n = 1$ je bezuvjetno sigurna od napada bilo kojeg individualnog korisnika.

Dokaz. Pretpostavimo da korisnik W želi odrediti ključ

$$K_{U,V} = a + b(r_U + r_V) + cr_U r_V \mod p,$$

gdje je $W \neq U, V$. Vrijednosti r_U i r_V su javne, ali a, b i c su nepoznati. Korisnik W zna vrijednosti

$$a_W = a + br_W \mod p,$$

i

$$b_W = b + cr_W \mod p,$$

jer su ovo koeficijenti polinomijalne funkcije $g_W(x)$ koje je povjerljivi autoritet poslao korisniku W.

Pokazat ćemo da korisnik W može odrediti nepoznate a, b i c, potrebne da izračuna $K_{U,V}$, jedino ako je vrijednost ključa $K^* \in \mathbb{Z}_p$ jednaka vrijednosti ključa $K_{U,V}$. Dobivamo sljedeće jednakosti:

$$a + b(r_U + r_V) + cr_U r_V = K^*,$$

$$a + br_W = a_W,$$

$$b + cr_W = b_W.$$

Prva jednakost predstavlja hipotezu da je $K_{U,V} = K^*$, dok druga i treća jednakost sadrže informaciju da su korisniku W poznati a, b i c iz $g_W(x)$. Kada bi ove jednakosti napisali matrično, determinanta bi bila oblika:

$$r_W^2 + r_U r_V - (r_U + r_V)r_W = (r_W - r_U)(r_W - r_V).$$

Determinanta je različita od nule jer je $r_W \neq r_U$, $r_W \neq r_V$ i p je prost. Imamo jedinstveno rješenje za a, b i c. Pokazali smo da W ne može izračunati $K_{U,V}$. To bi mogao jedino u slučaju da je $K^* = K_{U,V}$. □

Skup od dva korisnika, na primjer $\{W, X\}$ može odrediti ključ $K_{U,V}$, ako vrijedi da je $\{W, X\} \cap \{U, V\} = \emptyset$. Korisnici W i X znaju sljedeće:

$$a_W = a + br_W,$$

$$b_W = b + cr_W,$$

$$a_X = a + br_X,$$

i

$$b_X = b + cr_X.$$

Budući da imamo četiri jednadžbe sa tri nepoznanice, lako je izračunati jedinstveno rješenje za a, b i c. Kada su a, b i c poznati, može se kreirati polinomijalna funkcija $f(x, y)$ i izračunati bilo koji ključ.

Teorem 2. Bloomovu shemu predistribucije ključa za $n = 1$ može probiti skup bilo koja dva korisnika.

Bloomova shema predistribucije ključa se može generalizirati da bude sigurna od napada k korisnika. U tom slučaju polinomijalna funkcija $f(x, y)$ mora biti stupnja k. Povjerljivi autoritet koristi polinomijalnu funkciju f oblika

$$f(x, y) = \sum_{i=0}^{k} \sum_{j=0}^{k} a_{i,j} x^i y^j \mod p,$$

gdje je $a_{i,j} \in \mathbb{Z}_p$ $(0 \leq i \leq k, 0 \leq j \leq k)$, i $a_{i,j} = a_{j,i}$ za sve i, j. Primijetimo da je funkcija f simetrična.

Algoritam 3. Bloomova shema predistribucije ključa (za određeni n)

1. Prost broj p je javan i za svakog korisnika U, $r_U \in \mathbb{Z}_p$ je također javan. Elementi r_U moraju biti različiti.

2. Za sve i, j, povjerljivi autoritet bira slučajne elemente $a_{i,j} \in \mathbb{Z}_p$ tako da je $a_{i,j} = a_{j,i}$, za sve i, j. Povjerljivi autoritet kreira polinomijalnu funkciju f oblika:

$$f(x, y) = \sum_{i=0}^{k} \sum_{j=0}^{k} a_{i,j} x^i y^j \mod p.$$

3. Za svakog korisnika U, povjerljivi autoritet računa polinomijalnu funkciju:

$$g_U(x) = f(x, r_U) \mod p = \sum_{i=0}^{k} a_{U,i} x^i,$$

   i šalje vektor koeficijenata $(a_{U,0}, \ldots, a_{U,k})$ prema korisniku U preko sigurnog kanala.

4. Za bilo koja dva korisnika U i V, ključ je oblika: $K_{U,V} = f(r_U, r_V)$, gdje U računa

$$K_{U,V} = g_U(r_V)$$

   i V računa

$$K_{V,U} = g_V(r_U).$$

Bloomova shema predistribucije ključa zadovoljava sljedeće uvjete:

1. Niti jedan skup od k korisnika $W_1, \ldots, W_k$ ne može odrediti informacije o ključu $K_{U,V}$.
2. Bilo koji skup od $k+1$ korisnika $W_1, \ldots, W_{k+1}$ može probiti shemu.

Pretpostavimo da $k+1$ korisnika može razbiti shemu. Oni znaju polinomijalnu funkciju:

$$g_{W_i}(x) = f(x, r_{W_i}) \mod p,$$

gdje je $1 \leq i \leq k+1$.

Da bi ilustrirali napad potrebne su nam formule za polinomijalnu interpolaciju, dane u sljedeća dva teorema.

Teorem 3. Lagrangeova interpolacijska formula

Pretpostavimo da je p prost, a $x_1, x_2, \ldots, x_{m+1}$ su različiti elementi iz $\mathbb{Z}_p$, i pretpostavimo da su $a_1, a_2, \ldots, a_{m+1}$ također elementi (ne nužno različiti) iz $\mathbb{Z}_p$. Tada postoji jednistveni polinom $A(x) \in \mathbb{Z}_p[x]$ stupnja najviše m, tako da vrijedi $A(x_i) = a_i$, $1 \leq i \leq m+1$. $A(x)$ je oblika:

$$A(x) = \sum_{j=1}^{m+1} a_j \prod_{1 \leq h \leq m+1, h \neq j} \frac{x - x_h}{x_j - x_h}.$$

Teorem 4. Bivarijantna Lagrangeova interpolacijska formula

Pretpostavimo da je p prost, a $x_1, x_2, \ldots, x_{m+1}$ su različiti elementi iz $\mathbb{Z}_p$, i pretpostavimo da su $a_1(x), a_2(x), \ldots, a_{m+1}(x) \in \mathbb{Z}_p[x]$, stupnja najviše m. Tada postoji jednistveni polinom $A(x, y) \in \mathbb{Z}_p[x, y]$, stupnja najviše m, tako da vrijedi $A(x, y_i) = a_i(x)$, $1 \leq i \leq m+1$. Polinom $A(x, y)$ je oblika:

$$A(x, y) = \sum_{j=1}^{m+1} a_j(x) \prod_{1 \leq h \leq m+1, h \neq j} \frac{y - y_h}{y_j - y_h}.$$

Primjer 3. Bivarijantna Lagrangeova interpolacija

Pretpostavimo da je $p = 13$, $m = 2$, $y_1 = 1$, $y_2 = 2$, $y_3 = 3$,

$$a_1(x) = 1 + x + x^2,$$

$$a_2(x) = 7 + 4x^2,$$

i

$$a_3(x) = 2 + 9x.$$

Tada je

$$\frac{(y-2)(y-3)}{(1-2)(1-3)} = 7y^2 + 4y + 3,$$

$$\frac{(y-1)(y-3)}{(2-1)(2-3)} = 12y^2 + 4y + 10,$$

i

$$\frac{(y-1)(y-2)}{(3-1)(3-2)} = 7y^2 + 5y + 1.$$

Slijedi

$$A(x,y) = (1+x+x^2)(7y^2+4y+3)+(7+4x^2)(12y^2+4y+10)+(2+9x)(7y^2+5y+1) \mod 13$$

$$= y^2 + 3y + 10 + 5xy^2 + 10xy + 12x + 3x^2y^2 + 7x^2y + 4x^2.$$

Lako se može pokazati da je $A(x,i) = a_i(x)$, $i = 1, 2, 3$. Na primjer, kada je $i = 1$, imamo

$$A(x,1) = 1 + 3 + 10 + 5x + 10x + 12x + 3x^2 + 7x^2 + 4x^2 \mod 13$$

$$= 14 + 27x + 14x^2 \mod 13$$

$$= 1 + x + x^2.$$

Treba pokazati je li Bloomova shema predistribucije ključa nesigurna ako imamo $k + 1$ protivnika. Skup od $k + 1$ protivnika $W_1, \ldots, W_{k+1}$, zna $k + 1$ polinomijalnih funkcija stupnja k, oblika

$$g_{W_i}(x) = f(x, r_{W_i}) \mod p,$$

gdje je $1 \leq i \leq k + 1$.

Koristeći bivarijantnu interpolacijsku formulu, može se izračunati $f(x, y)$ (napravljeno u Primjeru 3.), i nakon toga ključ $K_{U,V}$.

Može se pokazati da je Bloomova shema predistribucije ključa sigurna od napada skupa k protivnika. Skup od k protivnika kolektivno zna k polinomijalnih funkcija stupnja k, oblika

$$g_{W_i}(x) = f(x, r_{W_i}) \mod p,$$

gdje je $1 \leq i \leq k+1$.

Neka je K bilo koji ključ čija je vrijednost nepoznata skupu protivnika, i neka je K^* proizvoljan ključ. Pokazat će se da postoji simetrična polinomijalna funkcija $f^*(x, y)$ koja je konzistentna sa informacijama poznatim skupu k protivnika i takva da je tajni ključ povezan sa $f^*(x, y)$ upravo K^*. Skup k protivnika ne može izostaviti niti jednu moguću vrijednost ključa. Definiramo:

$$f^*(x, y) = f(x, y) + (K^* - K) \prod_{1 \leq i \leq k} \frac{(x - r_{W_i})(y - r_{W_i})}{(r_U - r_{W_i})(r_V - r_{W_i})}.$$

Slijede neka svojstva od $f^*(x, y)$:

1. Funkcija f^* je simetrična polinomijalna funkcija, jer je f simetrična i produkt u prethodnoj jednakosti je također simetričan po x i y.

2. Za $1 \leq i \leq k$ vrijedi:

   $$f^*(x, r_{W_i}) = f(x, r_{W_i}) = g_{W_i}(x).$$

   To je zato jer svaki produkt u jednakosti za $f^*(x, y)$ sadrži izraz jednak nuli kada je $Y = r_{W_i}$ i tada je ukupni produkt jednak nuli.

3. Naposljetku,

   $$f^*(r_U, r_V) = f(r_U, r_V) + K^* - K = K^*,$$

   jer je produkt u jednakosti za $f^*(x, y)$ jednak 1.

Na temelju ovih svojstava zaključujemo da za svaku moguću vrijednost ključa K^*, postoji simetrična polinomijalna f^* takva da je $f^*(U, V) = K^*$ i tajna informacija koju čuva k protivnika je ostala nepromijenjena. Dokazali smo sljedeći teorem.

Teorem 5. Bloomova shema predistribucije ključa je bezuvjetno sigurna od napada bilo kojih k protivnika. Ali, bilo kojih $k+1$ protivnika može probiti shemu.

Bloomova shema predistribucije ključa je optimalna u pogledu prostora za pohranu. Dokazano je da bilo koja bezuvjetno sigurna predistribucija ključa koja je sigurna protiv skupa od k protivnika zahtjeva da prostor za pohranu svakog korisnika treba biti najmanje $k+1$ puta veći od duljine ključa.

5. Uzorci distribucije ključa

Pretpostavimo da imamo povjerljivi autoritet i mrežu sa n korisnika koje ćemo označiti sa $\mathcal{U} = \{U_1, \ldots, U_n\}$. Povjerljivi autoritet odabire v slučajnih ključeva $k_1, \ldots, k_v \in \mathcal{K}$, gdje je $\mathcal{K}$ aditivna Abelova grupa. Povjerljivi autoritet svakom korisniku daje (različit) podskup ključeva.

Definicija 1. Uzorak distribucije ključa je $v \times n$ matrica incidencije M sa elementima iz $\{0, 1\}$. Matrica M prikazuje koji ključevi će pripasti pojedinim korisnicima. Korisniku U_j je dan ključ k_i ako i samo ako je $M[i, j] = 1$, gdje je s $M[i, j]$ označen element koji se nalazi u presjeku i-tog retka i j-tog stupca matrice M.

Za uzorak distribucije ključa M i podskup korisnika $P \subseteq \mathcal{U}$, definiramo

$$keys(P) = \{i : M[i, j] = 1, \forall U_j \in P\}.$$

Skup $keys(P)$ sadrži indekse ključeva koji se nalaze kod svih korisnika iz P. Primjetimo da je

$$keys(P) = \bigcap_{U_j \in P} keys(U_j),$$

pri čemu smo s $keys(U_j)$ označili skup indeksa ključeva koji se nalaze kod korisnika U_j. Ako vrijedi da je $keys(P) \neq \emptyset$, tada je grupa ključeva za podskup P definirana s

$$k_P = \sum_{i \in keys(P)} k_i,$$

gdje se suma računa koristeći operaciju "$+$" definiranu u grupi $\mathcal{K}$. Svi članovi skupa P mogu izračunati grupni ključ k_P, bez komunikacije sa povjerljivim autoritetom. Grupa se najčešće sastoji od dva korisnika, ali opisan sustav dopušta i grupu ključeva koja se sastoji od više korisnika.

Primjer 4. Pretpostavimo da je $n = 4$, $v = 6$ i matrica M je oblika

$$\begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

Tada imamo:

$$keys(U_1) = \{1, 2, 3\},$$
$$keys(U_2) = \{1, 4, 5\},$$
$$keys(U_1, U_2) = \{1\}.$$

Slijedi da je $k_{\{U_1,U_2\}} = k_1$.

Da bi shema bila sigurna od protivnika, M mora zadovoljavati određena svojstva. Pretpostavimo da je P podskup korisnika koji posjeduju grupni ključ k_P i pretpostavimo da je F skup protivnika koji želi izračunati k_P na način da sazna sve informacije koje zna P. Pretpostavit ćemo i da je $F \cap P = \emptyset$, jer ako postoji korisnik $U_i \in P \cap F$, tada U_i odmah može izračunati k_P. Skup protivnika F može izračunati k_P ako je zadovoljen sljedeći uvjet:

$$keys(P) \subseteq \bigcup_{U_j \in F} keys(U_j).$$

To se lako vidi jer F drži sve ključeve pomoću kojih je moguće izračunati k_P. Ako uvjet ne vrijedi, tada postoji element

$$i \in keys(P) \setminus \left(\bigcup_{U_j \in F} keys(U_j) \right).$$

Vrijednost od k_P je suma izraza, od kojih je jedan k_i. Budući da vrijednost od k_i nije poznata skupu protivnika F, slijedi da F nema informacija o vrijednosti grupnog ključa k_P.

Metoda korištena u prethodnom primjeru može se lako generalizirati. Uvijek je moguće konstruirati $\binom{n}{2} \times n$ matricu M, u kojoj bilo koja dva korisnika u uzorku distribucije ključa imaju točno jedan zajednički ključ, a svaki ključ je poznat skupu od točno dva korisnika. Grupni ključ za bilo koja dva korisnika je jedinstveni ključ koji oboje posjeduju. U uzorku distribucije ključa postoji $\binom{n}{2}$ grupnih ključeva, i svaki korisnik mora pohraniti $n-1$ ključeva. Svaki grupni ključ $k_{\{U_j,U_j'\}}$ je siguran od skupa $\mathcal{U} \setminus \{U_j, U_j'\}$ svih ostalih korisnika (ovaj skup ima $n-2$ članova).

Općenito, želimo konstuirati uzorak distribucije ključa u kojem je broj ključeva pohranjen kod svakog korisnika pojedinačno najmanji mogući. Prethodni primjer omogućuje maksimalnu sigurnost, ali zahtjeva mnogo prostora za pohranu. Nekad je moguće reducirati potrebe za prostorom za pohranu ako sigurnosni uvjeti nisu striktni. Slično Bloomovoj shemi predistribucije ključa, možemo pretpostaviti scenarij u kojem se traži sigurnost samo protiv skupa određene veličine. Ilustrirajmo ovaj problem sljedećim primjerom:

Primjer 5. Pretpostavimo da je $n = 7$, $v = 7$ i matrica M je oblika

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

Tada imamo:

$$keys(U_1) = \{1, 4, 6, 7\},$$

$$keys(U_2) = \{1, 2, 5, 7\},$$

i

$$keys(U_1, U_2) = \{1, 7\}.$$

Slijedi da je $k_{\{U_1,U_2\}} = k_1 + k_7$.

Niti jedan drugi korisnik ne zna i k_1 i k_7, pa je grupni ključ $k_{\{U_1,U_2\}}$ siguran od napada bilo kojeg individualnog korisnika. U ovom primjeru, svaki par korisnika može izračunati ključ koji je siguran od napada bilo kojeg individualnog korisnika. Ukupno je moguće kreirati $\binom{7}{2} = 21$ grupni ključ za parove korisnika. Povjerljivi autoritet je ukupno poslao 7 ključeva, a svaki korisnik mora pohraniti 4 ključ, što je manje od $n - 1 = 6$ ključeva koji se moraju pohraniti u 'trivijalnoj' shemi.

5.1. Fiat - Naor uzorci distribucije ključa

Ova shema omogućava određivanje grupnog ključa za proizvoljan podskup korisnika na mreži. Odaberemo broj w gdje je $1 \leq w \leq n$ (w je sigurnosni parametar). Broj ključeva v određujemo prema sljedećoj formuli:

$$v = \sum_{i=0}^{w} \binom{n}{i}.$$

Fiat-Naor w-uzorak distribucije ključa je $v \times n$ matrica M, u kojoj svaki redak ima najmanje $n - w$ jedinica, što znači da svaki ključ posjeduje najmanje $n - w$ korisnika.

Ako imamo Fiat - Naor w-uzorak distribucije ključa, lako je vidjeti da postoji grupni ključ za svaki $P \subseteq U$, koji je siguran od bilo kojeg skupa protivnika F veličine najviše w. Ovo je lako dokazati, kako slijedi $|F| \leq w$, pa $|U \setminus F| \geq n - w$. Postoji ključ k_i dan

samo korisnicima iz $U \setminus F$. Za skup P vrijedi: $P \subseteq (U \setminus F)$, tako da svi korisnici iz P imaju ključ k_i i nijedan korisnik iz F nema k_i. Uvjet

$$keys(P) \subseteq \bigcup_{U_j \in F} keys(U_j)$$

nije zadovoljen.

Primjer 6. Pretpostavimo da je $n = 6$ i $w = 1$. Fiat - Naor 1-uzorak distribucije ključa ima $v = 7$ i uzorak distribucije ključa M je oblika

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Pretpostavimo da imamo podskup korisnika $P = \{U_1, U_3, U_4\}$. Tada imamo:

$$keys(U_1) = \{1, 2, 3, 4, 5, 6\},$$

$$keys(U_3) = \{1, 2, 3, 4, 6, 7\},$$

$$keys(U_4) = \{1, 2, 3, 5, 6, 7\},$$

i

$$keys(U_1, U_3, U_4) = \{1, 2, 3, 6\}.$$

Slijedi da je $k_{\{U_1,U_3,U_4\}} = k_1 + k_2 + k_3 + k_6$ i niti jedan drugi individualni korisnik ne može izračunati taj ključ.

5.2. Mitchell - Piper uzorci distribucije ključa

U ovom obliku uzoraka distribucije ključa, za svaki podskup od točno t članova postoji grupni ključ. Grupni ključ je potreban kako bi postojala sigurnost od napada skupa protivnika veličine w. Od posebnog je interesa slučaj kada je $t = 2$, jer to je slučaj kada se ključevi odnose na parove korisnika.

Definicija 2. Sustav skupova je uređeni par $(X, \mathcal{A})$, gdje je X konačan skup elemenata (točaka), i $\mathcal{A}$ je skup podskupova od X (blokova). Neka je $X = \{x_1, \ldots, x_v\}$ i $\mathcal{A} = \{A_1, \ldots, A_n\}$. Kažemo da je sustav skupova $(X, \mathcal{A})$ (t, w) - pokrivačka familija u kojoj za svaka dva disjunktna podskupa $P, F \subseteq \mathcal{A}$, gdje je $|P| = t$ i $|F| = w$, vrijedi da je

$$\bigcap_{A_i \in P} A_i \nsubseteq \bigcup_{A_j \in F} A_j.$$

(t, w) - pokrivačka familija se označava kao (t, w) - CFF (v, n) ako je $|X| = v$ i $|\mathcal{A}| = n$.

Presjek t blokova u (t, w) - pokrivačkoj familiji nije sadržan u uniji nikojih preostalih w blokova. Matrica incidencije od $(X, \mathcal{A})$ je $v \times n$ matrica $M = (m_{i,j})$ u kojoj je $m_{i,j} = 1$, ako je $x_i \in A_j$, a inače je 0.

Mitchell - Piper (t, w) - uzorak distribucije ključa je uzorak distribucije ključa u kojem postoji ključ za svaku skupinu od t korisnika, i svaki takav ključ je siguran od disjunktne suradnje najviše w protivnika.

Teorem 6. Pretpostavimo da je M $v \times n$ uzorak distribucije ključa. Tada je M (t, w) - uzorak distribucije ključa ako i samo ako je M matrica incidencije od (t, w) - pokrivačke familije (v, n).

Lako se primijeti da blokovi pokrivačke familije odgovaraju stupcima u M. Na primjer, stupci matrice incidencije M u Primjeru 5. tvore $(2, 1) - CFF(7, 7)$, $(X, \mathcal{A})$ gdje je

$$X = \{1, ..., 7\},$$

$$\mathcal{A} = \{\{1, 4, 6, 7\}, \{1, 2, 5, 7\}, \{1, 2, 3, 6\}, \{2, 3, 4, 7\},$$

$$\{1, 3, 4, 5\}, \{2, 4, 5, 6\}, \{3, 5, 6, 7\}\}.$$

6. Sheme distribucije ključa određenog razdoblja

U shemi distribucije ključa određenog razdoblja, povjerljivi autoritet bira tajne ključeve određenog razdoblja i prenosi ih mrežom na zahtjev korisnika u šifriranom obliku. Sa K_{Alice} označit ćemo Alicin tajni ključ i sa K_{Bob} označit ćemo Bobov tajni ključ. U nastavku slijede najvažnije sheme distribucije ključa određenog razdoblja.

6.1. Needham - Schroederova shema

Najprije ćemo algoritmom ilustrirati kako ova shema radi na algoritmu.

Algoritam 4. Needham - Schroederova shema

1. Alice bira slučajan broj r_A, i šalje $ID(Alice)$, $ID(Bob)$ i r_A povjerljivom autoritetu. Alicin identitet je označen sa $ID(Alice)$, a Bobov identitet je označen sa $ID(Bob)$.

2. Povjerljivi autoritet bira ključ određenog razdoblja koji ćemo označiti s K. Zatim određuje
$$t_{Bob} = e_{K_{Bob}}(K||ID(Alice)),$$
i
$$y_1 = e_{K_{Alice}}(r_A||ID(Bob)||K||t_{Bob}),$$
i šalje y_1 Alice. Sa t_{Bob} ili 'ticket to Bob' je označena poruka u kojoj se nalazi ključ K određenog razdoblja i Alicin identitet, a šifrirani su pomoću Bobovog ključa K_{Bob}. Sa y_1 je označena poruka koja u sebi sadrži r_A, $ID(Bob)$, K i t_{Bob}, a šifrirana je pomoću Alicina tajnog ključa K_{Alice}. Sa $||$ je označena operacija ulančavanja.

3. Alice dešifrira y_1 koristeći K_{Alice}, te tako saznaje K i t_{Bob}. Zatim Alice šalje Bobu t_{Bob}.

4. Bob dešifrira t_{Bob} sa svojim ključem K_{Bob}, i saznaje K. Bob bira slučajan broj r_B, i računa $y_2 = e_K(r_B)$. Zatim šalje Alice y_2.

5. Alice dešifrira y_2 koristeći ključ određenog razdoblja K, te saznaje r_B. Alice računa $y_3 = e_K(r_B - 1)$ i šalje y_3 Bobu.

Provjerimo sada ispravnost prethodno opisane sheme:

1. Kada Alice dešifrira y_1, provjerava je li otvoreni tekst $d_{K_{Alice}}(y_1)$ oblika

$$r_A||ID(Bob)||K||t_{Bob},$$

za neki K i t_{Bob}. Ako vrijedi gornji uvjet, Alice prihvaća, a u protivnom odbija postupak.

2. Kada Bob dešifrira y_3, provjerava da li otvoreni tekst zadovoljava

$$d_K(y_3) = r_B - 1.$$

Ako da, onda odobrava postupak.

Sažetak glavnih koraka sheme

U koraku 1, Alice traži od povjerljivog autoriteta ključ određenog razdoblja kako bi mogla komunicirati sa Bobom. U tom trenutku, moguće je da Bob uopće ne zna za Alicin zahtjev. U koraku 2, povjerljivi autoritet šalje Alice šifrirani ključ određenog razdoblja, a u koraku 3, Alice šalje Bobu šifrirani ključ određenog razdoblja. Svrha koraka 4 i 5 je uvjeriti Boba da Alice posjeduje ključ K određenog razdoblja. Alice koristi K kako bi saznala r_B i za šifriranje $r_B - 1$. Bob dešifrirajući y_3, provjerava da li Alice posjeduje ključ K određenog razdoblja. Ovaj proces se zove potvrda ključa.

6.2. Denning - Saccov napad na Needham - Schroederovu shemu

Pretpostavimo da neprijateljska treća strana, koju ćemo nadalje zvati Oscar, nadzire komunikaciju između Alice i Boba koja traje određeno razdoblje, koje ćemo označiti sa $\mathcal{S}$ i otkrije ključ K određenog razdoblja. Ovaj napad se zove napad poznatim ključem određenog razdoblja. Oscar može inicirati novu komunikaciju s Bobom (u određenom razdoblju koje ćemo označiti sa $\mathcal{S}'$), tako da mu pošalje prethodno korišten t_{Bob}. Njihova komunikacija opisana je algoritmom, počevši s trećim korakom.

Primijetimo da kada Bob odgovara sa $e_K(r'_B)$, Oscar to može dešifrirati koristeći poznat ključ K, oduzeti 1, i šifrirati rezultat. Vrijednost $e_K(r'_B - 1)$ je poslana Bobu u zadnjem toku određenog razdoblja $\mathcal{S}'$. Bob će to dešifrirati i prihvatiti.

Pogledajmo posljedice ovog napada. Na kraju određenog razdoblja $\mathcal{S}'$ između Oscara i Boba, Bob misli da ima "novi" ključ K određenog razdoblja koji je razmijenio sa Alice (to je zato jer se $ID(Alice)$ pojavljuje u t_{Bob}). Taj ključ K je poznat Oscaru, ali ne mora biti poznat Alice, jer je Alice možda bacila ključ K nakon prošlog razdoblja sa Bobom, npr. određenog razdoblja $\mathcal{S}$. Postoje dva načina na koje Bob može biti obmanut ovim napadom:

1. Ključ distribuiran u određenom razdoblju $\mathcal{S}'$ nije poznat Bobovom partneru Alice.

2. Ključ određenog razdoblja $\mathcal{S}'$, poznat je nekome tko nije Bobov partner (npr. Oscaru).

6.3. Kerberos

Kerberos je sustav zaštite podataka razvijen na MIT-u (Massachusetts Institute of Technology) kasnih osamdesetih i ranih devedesetih godina prošlog stoljeća, i obuhvaća seriju shema distribucije ključa. U sljedećem algoritmu opisana je jedna verzija sheme distribucije ključa.

Sa L ćemo označiti vremenski period u kojem bi informacija trebala ostati tajna. Na primjer, savjet za kupnju određene dionice mora ostati tajan nekoliko minuta dok državne tajne moraju ostati neotkrivene neograničeno dugo.

Algoritam 5. Pojednostavljeni Kerberos

1. Alice na slučajan način bira broj r_A, i povjerljivom autoritetu šalje $ID(Alice)$, $ID(Bob)$ i r_A.

2. Povjerljivi autoritet bira ključ K određenog razdoblja i period validacije L. Zatim određuje
$$t_{Bob} = e_{K_{Bob}}(K||ID(Alice)||L),$$
i
$$y_1 = e_{K_{Alice}}(r_A||ID(Bob)||K||L).$$
Povjerljivi autoritet šalje Alice y_1 i t_{Bob}.

3. Alice dešifrira y_1 koristeći K_{Alice}, te saznaje K. Zatim određuje trenutno vrijeme $time$ i
$$y_2 = e_K(ID(Alice)||time).$$
Alice šalje Bobu t_{Bob} i y_2.

4. Bob dešifrira t_{Bob} koriteći svoj ključ K_{Bob}, te saznaje K. Također dešifrira y_2, koristeći ključ K, i saznaje $time$. Zatim određuje
$$y_3 = e_K(time + 1).$$
Bob Šalje Alice y_3.

Provjera ispravnosti prethodno opisane sheme:

1. Kada Alice dešifrira y_1, provjerava je li otvoreni tekst $d_{K_{Alice}}(y_1)$ oblika

$$d_{K_{Alice}}(y_1) = r_A||ID(Bob)||K||L,$$

za neki K i L. Ako vrijedi gornji uvjet, Alice prihvaća, a u protivnom odbija postupak.

2. Kada Bob dešifrira t_{Bob} i y_2, provjerava je li otvoreni tekst $d_K(y_2)$ oblika

$$d_K(y_2) = ID(Alice)||time,$$

i otvoreni tekst oblika

$$d_{K_{Bob}}(t_{Bob}) = K||ID(Alice)||L,$$

gdje je $ID(Alice)$ isti u oba otvorena teksta i $time \leq L$. Ako vrijede ovi uvjeti, onda Bob prihvaća postupak, a u suprotnom ga odbija.

3. Kada Alice dešifrira y_3, provjerava je li $d_K(y_3) = time + 1$. Ako vrijedi gornji uvjet, Alice prihvaća, a u protivnom odbija postupak.

Sažetak sheme

Kada Alice šalje zahtjev za ključ određenog razdoblja povjerljivom autoritetu, povjerljivi autoritet na slučajan način generira novi ključ K određenog razdoblja. Povjerljivi autoritet odmah određuje i vrijeme trajanja novog ključa K, koje ćemo označiti s L. Sve ove informacije se šifriraju prije nego li se pošalju Alice. Alice može koristiti svoj tajni ključ za dešifriranje poruke y_1 i na taj način otkriva K i L. Potvrdit će da je trenutno vrijeme unutar vremena trajanja ključa i da poruka y_1 sadrži r_A i $ID(Bob)$. Ove provjere sprječavaju Oscara da ponavlja staru poruku y_1, koju je povjerljivi autoritet slao u nekom prošlom razdoblju. Alice će Bobu poslati t_{Bob}, a pomoću novog ključa K određenog razdoblja šifrirat će trenutno vrijeme i $ID(Alice)$, i tu poruku y_2 poslati Bobu. Kada Bob primi y_2 i t_{Bob} od Alice, dešifrira t_{Bob} da otkrije K, L i $ID(Alice)$. Tada koristi novi ključ K određenog razdoblja za dešifriranje poruke y_2, i potvrđuje da su $ID(Alice)$ (dešifriran iz t_{Bob}) i y_2 isti. To osigurava Bobu da je ključ određenog razdoblja šifriran unutar t_{Bob} isti ključ koji se koristio za šifriranje y_2. Također treba provjeriti da je $time \leq L$, čime se može uvjeriti da ključ K nije istekao. Na kraju, Bob šifrira $time + 1$ koristeći novi ključ K određenog razdoblja i šalje rezultat natrag Alice. Kada Alice primi poruku, y_3, dešifrira ju koristeći K i provjerava je li rezultat $time + 1$. To uvjerava Alice da je ključ K određenog razdoblja uspješno poslan Bobu, jer je potreban da kreira poruku y_3. Svrha vremena trajanja L je spriječiti aktivnog

protivnika od čuvanja starih poruka koje bi mogao slati kasnije. Svi korisnici u mreži bi trebali imati usklađene satove, jer trenutno vrijeme određuje je li ključ K određenog razdoblja valjan ili ne. U praksi je vrlo teško postići savršenu sinkronizaciju, pa male varijacije u vremenu moraju biti dopuštene.

Usporedba Needham - Schroederove sheme i Kerberosa

1. U Kerberosu, obostrana potvrda ključa ostvarena je u trećem i četvrtom koraku algoritma. Koristeći novi ključ K određenog razdoblja za šifriranje $ID(Alice)$, Alice pokušava uvjeriti Boba da ona zna vrijednost od K. Slično, kada Bob šifrira $time + 1$ koristeći K, pokazuje Alice da zna vrijednost od K.

2. U Needham - Schroederovoj shemi, informacije namijenjene Bobu su dva puta šifrirane: t_{Bob} koji je već šifriran, ponovno je šifriran koristeći tajni ključ od Alice. Za ovaj postupak se smatra da nema korisnu svrhu i da čini shemu nepotrebno kompleksnom. Kerberos ne koristi dvostruko šifriranje.

3. Djelomična zaštita od Denning - Saccovog napada je osigurana u Kerberosu potvrdom da je trenutno vrijeme unutar vremena trajanja L. Ovo ograničava vremenski period u kojem Denning - Saccov napad može biti izvršen.

Needham - Schroederova shema i Kerberos imaju neka svojstva koja su potrebna i korisna u realnoj upotrebi sheme distribucije ključa određenog razdoblja:

1. Sheme koje koriste vremenske oznake zahtjevaju pouzdane i sinkronizirane satove. Teške su za analiziranje i zbog toga se, ako je moguće, ne preporučuje korištenje vremenskih oznaka (nego slučajnih izazova).

2. Potvrda ključa nije nužno važan atribut sheme distribucije ključa određenog razdoblja. Npr. posjedovanje ključa za vrijeme trajanja komunikacije u shemi distribucije ključa određenog razdoblja ne implicira posjedovanje ključa kasnije, kada će se ustvari i koristiti. Iz tog razloga često se preporučuje da se potvrda ključa u shemi distribucije ključa određenog razdoblja izostavi.

3. U Needham - Schroederovoj shemi i Kerberosu, šifriranje se koristi da osigura sigurnost i autentikaciju. Na primjer, u drugom koraku Needham - Schroederove sheme mogli smo izostaviti dvostruko šifriranje i koristiti autentikaciju poruke (MAC - to je kontrolni iznos koji koristi ključ određenog razdoblja kako bi otkrio slučajne ili namjerne promjene na podacima). Povjerljivi autoritet na slučajan način bira ključ K određenog razdoblja i tada računa:

$$y_1 = (e_{K_{Bob}}(K), MAC_{Bob}(ID(Alice)||e_{K_{Bob}}(K))),$$

i

$$y_1' = (e_{K_{Alice}}(K), MAC_{Alice}(ID(Bob)||r_A||e_{K_{Alice}}(K))).$$

Povjerljivi autoritet će slati y_1 i y_1' Alice koja će tada povjeriti y_1 Bobu.

4. Da bi se izbjegao Denning - Saccov napad, struktura toka sheme mora se modificirati. Bilo koja sigurna shema mora uključiti Boba kao aktivnog sudionika prije nego što primi ključ određenog razdoblja, da spriječi ponovljeni Denning - Saccov napad. Rješenje predlaže da Alice kontaktira Boba prije slanja zahtjeva za ključ određenog razdoblja povjerljivom autoritetu.

6.4. Bellare - Rogawayova shema

Opis sheme započinjemo algoritmom.

Algoritam 6. Bellare - Rogawayova shema distribucije ključa određenog razdoblja

1. Alice na slučajan način bira broj r_A, i šalje Bobu $ID(Alice)$, $ID(Bob)$ i r_A.

2. Bob na slučajan način bira broj r_B, i šalje $ID(Alice)$, $ID(Bob)$, r_A i r_B povjerljivom autoritetu.

3. Povjerljivi autoritet na slučajan način bira ključ K određenog razdoblja. Tada računa

$$y_B = (e_{K_{Bob}}(K), MAC_{Bob}(ID(Alice)||ID(Bob)||r_B||e_{K_{Bob}}(K))),$$

i

$$y_A = (e_{K_{Alice}}(K), MAC_{Alice}(ID(Bob)||ID(Alice)||r_A||e_{K_{Alice}}(K))).$$

Povjerljivi autoritet šalje Bobu y_B i Alice y_A.

Prethodni algoritam ima drugačiju strukturu toka od shema koje smo do sada promatrali. Alice i Bob na slučajan način biraju izazove, koji se šalju povjerljivom autoritetu. Bob je uključen u shemu prije nego povjerljivi autoritet šalje ključ određenog razdoblja. Informacije koje povjerljivi autoritet šalje Alice sastoje se od:

1. Ključa određenog razdoblja (šifriran koristeći tajni ključ od Alice),

2. Autentikacije poruke za šifrirani ključ određenog razdoblja, identiteta Alice i Boba i Alicinog izazova.

Informacije poslane Bobu su analogne. Alice i Bob će prihvatiti postupak ako su njihove autentikacije poruka valjane. Npr. kada Bob primi šifrirani ključ određenog razdoblja, npr. $y_{B,1}$, i autentikaciju poruke, npr. $y_{B,2}$, on potvrđuje da vrijedi

$$y_{B,2} = MAC_{Bob}(ID(Alice)||ID(Bob)||r_B||y_{B,1}).$$

Primijetimo da u ovoj shemi nije proveden postupak potvrde ključa. Kada Alice prihvaća postupak, ona ne zna je li ga i Bob prihvatio i da li je uopće Bob dobio poruku koju je poslao povjerljivi autoritet. Kada Alice prihvaća postupak, to samo znači da je primila informaciju koju je očekivala i da je ta informacija valjana (ili preciznije, da je autentikacija poruke valjana). Iz Alicine perspektive, kada ona prihvati postupak, ona vjeruje da je primila novi ključ određenog razdoblja od povjerljivog autoriteta. Budući da je ključ određenog razdoblja šifriran pomoću Alicina tajnog ključa, ona je sigurna da nitko drugi nije izračunao ključ K određenog razdoblja iz informacija koje je ona upravo primila. Bob je također trebao dobiti šifrat istog ključa određenog razdoblja. Alice može biti sigurna da nitko drugi osim Boba ne može izračunati novi ključ određenog razdoblja. Analiza je slična kada se čitav postupak pogleda s Bobove strane. Drugim riječima, umjesto potvrde ključa, dovoljan uvjet sigurnosti je da nitko osim partnera sudionika u shemi ne može izračunati novi ključ određenog razdoblja. Cilj napadača je da 'pošteni' sudionik sheme prihvati komunikaciju sa napadačem koji zna vrijednost ključa K određenog razdoblja. Npr. pretpostavimo da Alice nasjedne i prihvati postupak, a njen partner je Bob. Napadač Oscar postiže cilj ako može izračunati ključ K određenog razdoblja ili ako neki drugi korisnik na mreži (npr. Charlie) može izračunati ključ K određenog razdoblja. Oscarov napad neće biti uspješan ako je Alice jedini korisnik na mreži koji može izračunati ključ K određenog razdoblja.

U nastavku razmatramo jednu verziju sheme distribucije ključa određenog razdoblja u kojoj vrijedi sljedeća pretpostavka: ako Alice prihvati postupak, tada je vjerojatnost da netko drugi osim Boba zna ključ određenog razdoblja mala. Sada ćemo pokazati da je Bellare - Rogawayova shema distribucije ključa određenog razdoblja sigurna. Pretpostavka je da su Alice, Bob i povjerljivi autoritet pošteni, shema šifriranja i autentikacija poruke su sigurne i tajni ključ je poznat jedino njihovim vlasnicima,a slučajni izazovi se generiraju koristeći generatore slučajnih brojeva. Na kraju, pretpostavljamo da povjerljivi autoritet generira ključ određenog razdoblja koristeći savršen generator slučajnih brojeva.

Pogledajmo različite načine u kojima Oscar može izvršiti napad. Za svaku od ovih mogućnosti, vrijedi da Oscar neće biti uspješan osim sa malom vjerojatnošću. Ove mogućnosti nisu međusobno isključive.

1. Oscar je pasivan napadač.

2. Oscar je aktivan napadač i Alice je legitiman sudionik sheme. Oscar se može predstaviti kao Bob ili povjerljivi autoritet ili može presresti i promijeniti poruke poslane za vrijeme trajanja komunikacije između Alice i Boba.

3. Oscar je aktivan napadač i Bob je legitiman sudionik sheme. Oscar se može predstaviti kao Alice ili povjerljivi autoritet ili može presresti i promijeniti poruke poslane za vrijeme trajanja komunikacije između Alice i Boba.

Sada ćemo analizirati još neke moguće napade.

1. Ako je napadač pasivan, tada će Alice i Bob oboje prihvatiti bilo koji postupak u kojem sudjeluju. Oboje će moći dešifrirati isti ključ K određenog razdoblja. Nitko drugi neće moći izračunati ključ određenog razdoblja, jer je šifriranje sheme sigurno.

2. Pretpostavimo da je Alice legitiman sudionik sheme. Ona želi otkriti novi ključ određenog razdoblja koji će biti poznat samo Bobu i njoj. Alice ne zna da li uopće komuicira sa Bobom, jer se Oscar može lažno predstaviti kao Bob. Kada Alice primi poruku y_A, provjerava je li autentikacija poruke valjana. Autentikacija poruke uključuje r_A kao i identitete od Alice i Boba i šifriran ključ određenog razdoblja $e_{K_{Alice}}(K)$. To uvjerava Alice da je autentikacija poruke ponovno izračunata od povjerljivog autoriteta, jer je povjerljivi autoritet jedina strana osim Alice koja zna ključ MAC_{Alice}, dok r_A sprječava ponavljanje autentikacije poruke iz prethodnog razdoblja. Naposljetku, uključujući $e_{K_{Alice}}(K)$ u autentikaciji poruke sprječava napadača da zamijeni ključ određenog razdoblja sa nečim drugim. Alice može biti uvjerena da je Bob jedini korisnik koji može dešifrirati ključ K određenog razdoblja, iako se Oscar lažno predstavio kao Bob.

3. Pretpostavimo da je Bob legitiman sudionik sheme. On vjeruje da će otkriti novi ključ određenog razdoblja koji će biti poznat samo njemu i Alice. Bob ne zna da li uopće komuicira sa Alice jer se Oscar može lažno predstaviti kao Alice. Kada Bob primi poruku y_B, provjerava je li autentikacija poruke valjana. Autentikacija poruke uključuje r_B kao i identitete od Alice i Boba i šifriran ključ određenog razdoblja $e_{K_{Bob}}(K)$. Na taj način Bob može potvrditi da je autentikacija poruke ponovo izračunata od strane povjerljivog autoriteta, jer je povjerljivi autoritet jedina strana osim Boba koja zna ključ MAC_{Bob}. Uloga od r_B je da spriječi ponavljanje autentikacije poruke iz prethodne sesije. Naposljetku, uključivanje $e_{K_{Bob}}(K)$ u autentikaciju poruke sprječava napadača da zamijeni ključ određenog razdoblja sa nečim drugim. Bob može biti uvjeren da je Alice jedini korisnik koji može dešifrirati ključ K određenog razdoblja, iako se Oscar lažno predstavio kao Alice.

7. Zaključak

Cilj kriptografije je onemogućiti čitanje poruka svima kojima one nisu namijenjene. Ključ se koristi za šifriranje i dešifriranje poruka i zbog toga je važno da se on sigurno distribuira od pošiljatelja do primatelja. Protivnik koji sazna sadržaj ključa, lako će saznati i sadržaj poruke. Algoritam za distribuciju ključa mora biti siguran od napada protivnika, ne smije biti preskup, te mora biti optimalan u pogledu korištenja prostora za pohranu. Sve ove karakterisitke teško je pronaći u jednom algoritmu, pa je tako Diffie - Hellmanova predistribucija ključa sigurna samo u slučaju pasivnih napada. Bezuvjetno sigurna predistribucija ključa je preskupa, pa smo promatrali Bloomovu shemu predistribucije ključa koja je sigurna od napada skupa k protivnika i optimalna je u pogledu prostora pohrane. Zatim smo promatrali Fiat - Naor i Mitchell - Piper uzorke distribucije ključa koji koriste grupni ključ koji omogućuje sigurnost od napada skupa protivnika veličine w. Kerberos definira vremenski period L unutar kojeg bi informacija trebala ostati tajna.

Sigurnost je daleko najvažniji uvjet koji ovi algoritmi moraju ispuniti. To posebno vrijedi za velike sustave poput banaka, vlada i ostalih institucija koje čuvaju i razmjenjuju vrlo važne podatke. Takvi veliki sustavi mogu korisiti skuplje algoritme i one koji zahtjevaju više prostora za pohranu. Svakodnevnom komunikacijom korisnika na internetu ne razmjenjuju se tako važni podaci, ali takvih poruka ima mnogo više, pa se za zaštitu takve vrste komunikacije mogu koristiti manje 'sigurni' algoritmi s optimalnijim korištenjem prostora za pohranu.

Literatura

[1] A.J. MENEZES, P.C. VAN OORSCHOT, S.A. VANSTONE, *Handbook of applied cryptography*, CRC Press Book, Boca Raton, 1996.

[2] D.R. STINSON, *Cryptography Theory and practice (3ed)*, Chapman and Hall/CRC, Boca Raton, 2006.

8. Sažetak i ključne riječi

U ovom diplomskom radu predstavit ćemo najvažnije sheme distribucije ključa. Tri glavne sheme su: Shema predistribucije ključa, Shema distribucije ključa određenog razdoblja i Shema dogovora ključa. Zatim ćemo iz svake od skupine shema promatrati neke značajnije i analizirati koliko su sigurne u slučaju napada. Od shema predistribucije ključa, objasnit ćemo Diffie - Hellmanovu predistribuciju ključa i Bloomovu shemu predistribucije ključa. Od uzoraka distribucije ključa, promatrali smo Fiat - Naor i Mitchell - Piper uzorke distribucije ključa. Od shema distribucije ključa za određeno razdoblje, govorit ćemo o Needham - Scroederovoj shemi, Kerberosu i Bellare - Rogawayovoj shemi. Objasnit ćemo i Denning - Saccov napad na Needham - Schroederovu shemu.

Ključne riječi:

Shema predistribucije ključa, shema distribucije ključa za određeno razdoblje, shema dogovora ključa, Diffie - Hellmanova predistribucija ključa, Bloomova shema predistribucije ključa, Fiat - Naor i Mitchell - Piper uzorci distribucije ključa, Needham - Scroederova shema, Kerberos i Bellare - Rogawayova shema.

9. Title, summary and keywords

Title: Key distribution

Summary

In this work, we will present the most important Key distribution schemes. Three main schemes are: Key predistribution scheme, Session key distribution scheme and Key agreement scheme. Then we will observe the most significant schemes from each of the three main groups and analyse their security in case of attack. From the Key predistribution schemes, we will explain Diffie - Hellman key predistribution scheme and Bloom key predistribution scheme. Then we will say something about Key distribution patterns, and explain Fiat - Naor and Mitchell - Piper key distribution patterns. From Session key distribution schemes; Needham - Scroeder scheme, Kerberos and Bellare - Rogaway scheme will be explained. Also, we will present Denning - Sacco attack on Needham - Schroeder scheme.

Key words: Key predistribution scheme, session key distribution scheme, key agreement scheme, Diffie - Hellman key predistribution, Bloom key predistribution scheme, Fiat - Naor and Mitchell - Piper key distribution patterns, Needham - Scroeder scheme, Kerberos and Bellare - Rogaway scheme.

10. Životopis

Rođena sam 9.10.1984. godine u Zagrebu. Pohađala sam Osnovnu školu Matije Gupca i Privatnu klasičnu gimnaziju. Upisujem studij matematike na Prirodoslovno-matematičkom fakultetu, Sveučilišta u Zagrebu. Nakon završenog Preddiplomskog sveučilišnog studija matematike, školovanje nastavljam na Diplomskom studiju matematike, smjer Primijenjena matematika na PMF-u u Zagrebu, te potom na Diplomskom studiju matematike, smjer Financijska matematika i statistika na Sveučilištu J.J. Strossmayera u Osijeku.