



(12) Patentskrift

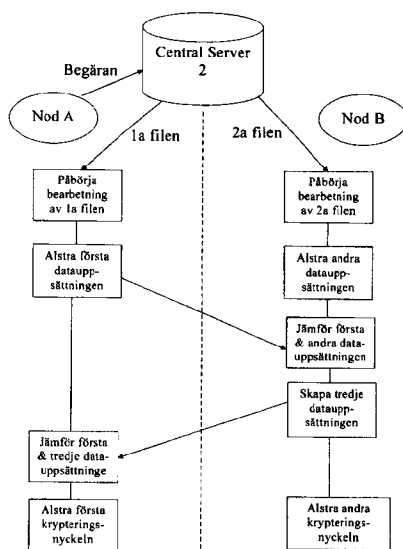
(10) SE 534 384 C2

(21) Patentansökningsnummer: 0900918-4
(45) Patent meddelat: 2011-08-02
(41) Ansökan allmänt tillgänglig: 2011-01-04
(22) Patentansökan inkom: 2009-07-03
(24) Löpdag: 2009-07-03
(83) Deposition av mikroorganism: ---
(30) Prioritetsuppgifter: ---

(51) Internationell klass:
H04L 9/08 (2006.01)

(73) Patenthavare: Kelisec AB, Björn Barkmans väg 2, 148 32 Ösmo SE
(72) Uppfinnare: Elise Revell, Ösmo SE
(74) Ombud: Groth & Co KB, Box 6107, 102 32 Stockholm SE
(54) Benämning: Förfarande för att alstra en krypterings-/dekrypteringsnyckel
(56) Anförda publikationer: ---
(47) Sammandrag:

Den föreliggande uppfinningen hänför sig till ett förfarande för att alstra en krypterings-/dekrypteringsnyckel och i synnerhet för att alstra en krypterings-/dekrypteringsnyckel av engångstyp som används för symmetrisk kryptering, dvs. där samma nyckel används både för kryptering och för dekryptering. För att starta nyckelalstringen skickar en första nod (A) en begäran till en central server (2) för att sätta upp förbindelse med en andra nod (2). Den centrala servern (2) skickar en nyckelalstringsfil till båda noderna (A och B). Varje nod alstrar en olik tillfällig datauppsättning, en första och andra datauppsättning. Den första datauppsättningen som alstras av den första noden (A) skickas till den andra noden (B), som baserad på denna datauppsättning alstrar en tredje datauppsättning som skickas tillbaka till den första noden. Alstringen av en första krypteringsnyckel i noden (A) baseras på en bit för bit jämförelse mellan den tredje och den första tillfälliga datauppsättningen och alstringen av en andra krypteringsnyckel baseras på en bit för bit jämförelse mellan den första och den andra tillfälliga datauppsättningen. Den första och den andra krypteringsnyckeln är desamma.



SAMMANDRAG

Den föreliggande uppfinningen hänför sig till ett förfarande för att alstra en krypterings-/dekrypteringsnyckel och i synnerhet för att alstra en krypterings-/dekrypteringsnyckel av engångstyp som används för symmetrisk kryptering, dvs. där samma nyckel används både för kryptering och för dekryptering. För att starta nyckelalstringen skickar en första nod (A) en begäran till en central server (2) för att sätta upp förbindelse med en andra nod (2). Den centrala servern (2) skickar en nyckelalstringsfil till båda noderna (A och B). Varje nod alstrar en olik tillfällig datauppsättning, en första och andra datauppsättning. Den första datauppsättningen som alstras av den första noden (A) skickas till den andra noden (B), som baserad på denna datauppsättning alstrar en tredje datauppsättning som skickas tillbaks till den första noden. Alstringen av en första krypteringsnyckel i noden (A) baseras på en bit för bit jämförelse mellan den tredje och den första tillfälliga datauppsättningen och alstringen av en andra krypteringsnyckel baseras på en bit för bit jämförelse mellan den första och den andra tillfälliga datauppsättningen. Den första och den andra krypteringsnyckeln är desamma.

Fig. 1

FÖRFARANDE FÖR ATT ALSTRA EN KRYPTERINGS- /DEKRYPTERINGSNYCKEL

5 **Tekniskt område**

Den föreliggande uppfinningen hänför sig till ett förfarande för att alstra en krypterings-/dekrypteringsnyckel och i synnerhet för att alstra en krypterings-/dekrypteringsnyckel av engångstyp som används för symmetrisk kryptering, dvs. där samma nyckel används både för kryptering och dekryptering. Den föreliggande uppfinningen avser vidare ett datorprogram som innefattar kod för att utföra förfarandet när det körs på en dator och en datorprogramprodukt som innefattar programkod som är lagrad på ett datorläsbart media för att utföra förfarandet, när produkten körs på en dator.

Bakgrund

15 Inom kryptografi är en nyckel ett stycke information som bestämmer det funktionella utdatat från en kryptoalgoritm. Utan en nyckel skulle algoritmen inte ha något resultat. Vid kryptering specificerar en nyckel den särskilda transformering som skall göras av klartext till krypterad text, eller tvärtom under dekrypteringen. Nycklar används också i andra kryptoalgoritmer, t.ex. digitala signaturer och meddelandeautentiseringskoder.

Vid design av säkerhetssystem är det alltid klokt att anta att detaljer hos kryptoalgoritmen redan är kända hos en möjlig intrångsgörare. Denna princip är känd som Kerckhoffs princip och sålunda är det bara nyckelns hemlighet som utgör säkerheten. Denna princip baserar sig på det faktum att det är svårt att undanhålla detaljer hos en vida spridd algoritmhemlighet. En nyckel är ofta enklare att skydda, eftersom den ofta består av en liten mängd information i jämförelse med krypteringsalgoritmen. Det kan emellertid också vara svårt att hålla en nyckel hemlig och om en angripare erhåller nyckeln på något sätt så kan han eller hon återskapa det ursprungliga meddelandet ur det krypterade datat.

30 Krypteringsalgoritmer som använder samma nyckel för både kryptering och dekryptering är såsom nämnts ovan kända under beteckningen symmetriska nyckelalgoritmer. Det finns också asymmetriska nyckelalgoritmer som använder nyckelpar, en för att kryptera och en för att dekryptera. Dessa asymmetriska nyckelalgoritmer möjliggör att en nyckel kan göras publik medan den privata nyckeln behålls på endast ett ställe. De är konstruerade så att de privata nycklarna är extremt svåra att komma åt även om motsvarande publika nyckel är känd. En användare av en publik nyckel kan

publicera sin publika nyckel samtidigt som han behåller sin privata nyckel hemlig, vilket möjliggör att alla kan sända ett krypterat meddelande till denna användare.

För att en nyckel skall betraktas som "säker" i samband med symmetriska krypteringsalgoritmer anses en längd på 80 bitar allmänt vara ett minimum och 128 bitars nycklar anses vanligtvis som mycket starka. Nycklarna som används vid kryptering med publika nycklar har någon matematisk struktur. Till exempel är de publika nycklar som används inom RSA-systemet produkten av två primtal. System som använder publika nycklar kräver därför större nyckellängder än symmetriska system för att få en liknande säkerhetsnivå. 3072 bitar föreslås som nyckellängd för system som baserar sig på utbrytnings- och diskreta heltalslogaritmer vars syfte är att ha en säkerhetsnivå som är likvärdig med ett 128 bitars symmetriskt chiffer.

Såsom nämnts ovan är det möjligt att alstra nycklar med en hög säkerhetsnivå om de är tillräckligt långa, både för nycklar baserade på symmetriska och asymmetriska algoritmer. Det finns emellertid ett problem vid nyckeldistributionen. Om t.ex. två parter önskar att kommunicera med varandra med användning av symmetriskt krypto måste de först bestämma vilken nyckel som skall användas och sedan distribuera den på ett säkert sätt från den ena parten till den andra. Nyckeln måste vidare hållas hemlig av båda parter. Risken att en inkräktare kan ta reda på nyckeln ökar med den tid som nyckeln används. Det är därför normalt att dessa endast är giltiga under en begränsad tid, t.ex. sex eller tolv månader. Efter denna tid måste en ny nyckel distribueras.

Också distributionen av nycklar med asymmetrisk kryptering har problem med nyckeldistributionen när två parter vill kommunicera med varandra. För att kunna sända information i båda riktningarna behöver de utbyta publika nycklar med varandra. Också i detta fall har nycklarna ofta en begränsad tidperiod under vilka de är giltiga. För en part som kommunicerar med många olika parter kan hanterandet och distributionen av giltiga publika nycklar vara enerverande. Ett typiskt exempel är att nyckelns giltighet har löpt ut när du behöver skicka någon hemlig information brådskande till en annan part eller att man ännu inte har utbytt publika nycklar.

En annan typ av kryptografi är kvantkryptering, som använder kvantmekanismer för att garantera säker kommunikation. Det möjliggör att två parter kan framställa en delad slumpmässig bitsträng som endast är känd av dem själva och som kan användas som nyckel för att kryptera och dekryptera meddelanden. En viktig och unik egenskap hos kvantkryptering är möjligheten för de två kommunicerande användarna att detektera närvaron av någon tredje part som försöker få reda på nyckeln. Detta är resultatet av en fundamental aspekt inom kvantmekaniken, dvs. processen att mäta ett

kvantsystem kommer att påverka systemet. Eftersom en tredje part försöker avlyssna nyckeln så måste de på något sätt mäta den och därigenom bli detekterbar. Säkerheten hos kvantkryptering vilar sålunda på grunderna inom kvantmekaniken i motsats till traditionell nyckelkryptering som förlitar sig på svårigheten att beräkna vissa matematiska funktioner och som inte kan ge några indikationer på avlyssning eller garantera nyckelsäkerhet.

Kvantkryptering används endast för att framställa och distribuera en nyckel och inte för att överföra något meddelandedata. Denna nyckel kan sedan användas för någon vald krypteringsalgoritm för att kryptera och dekryptera ett meddelande, som sedan kan sändas över en vanlig kommunikationskanal.

Även om nyckelalstringen vid kvantkryptering ger ett mycket säkert sätt att alstra och distribuera en nyckel har det också en påtaglig nackdel. Avståndet över vilken en kvantnyckel kan distribueras är begränsad till omkring 100 kilometer beroende på kvantmekanikens egenskaper.

I ljuset av ovannämnda problem finns ett behov för att på ett enkelt sätt alstra och distribuera en krypteringsnyckel.

Sammanfattning av uppfinningen

Problemet som den föreliggande uppfinningen avser lösa är att alstra en krypteringsnyckel, som inte behöver distribueras till noderna som vill kommunicera med varandra, dvs. där nyckeln kan alstras av noderna själva.

Enligt en första aspekt av uppfinningen löses detta problem av ett förfarande för att alstra en krypterings-/dekrypteringsnyckel, som är användbar för säker kommunikation mellan en första nod och en andra nod. Förfarandet innefattar stegen:

att sända en begäran från den första noden A till en central server för att sätta upp en förbindelse med den andra noden,

att från den centrala servern skicka en första nyckelalstrande fil till den första noden och andra nyckelalstrande fil till den andra noden i gensvar på begäran från den första noden,

bearbeta den första nyckelalstringsfilen vid den första noden och den andra nyckelalstringsfilen vid den andra noden,

alstra en första tillfällig datauppsättning vid den första noden och en andra tillfällig datauppsättning vid den andra noden,

skicka den första tillfälliga datauppsättningen från den första till den andra noden,

jämföra bitarna i den första tillfälliga datauppsättningen med motsvarande bitar i den andra tillfälliga datauppsättningen,

5 skapa en ny tredje tillfällig datauppsättning baserad på en bit för bit jämförelse mellan den första och den andra tillfälliga datauppsättningen genom att sätta ett första värde om det jämförda bitarna är lika och ett andra värde om de jämförda bitarna är olika,

skicka den tredje tillfälliga datauppsättningen från den andra noden till den första noden,

10 jämföra bitarna i den tredje tillfälliga datauppsättningen med motsvarande bitar i den första tillfälliga datauppsättningen,

alstra en första krypteringsnyckel baserad på en bit för bit jämförelse mellan den tredje och den första tillfälliga datauppsättningen genom att behålla värdet hos biten hos den första datauppsättningen om motsvarande bit hos den tredje tillfälliga datauppsättningen är satt till det första värdet och ignorera biten hos den första tillfälliga datauppsättningen om den motsvarande biten hos den tredje tillfälliga datauppsättningen är satt till det andra värdet,

alstra en andra krypteringsnyckel baserad på en bit för bit jämförelse mellan den första och den andra tillfälliga datauppsättningen genom att behålla värdet hos den bit av den andra datauppsättningen om motsvarande bit hos den första tillfälliga datauppsättningen är lika och ignorera denna bit hos den andra tillfälliga datauppsättningen om de jämförda bitarna är olika, varvid den första och den andra krypteringsnyckeln är desamma.

25 Enligt en andra aspekt av den föreliggande uppfinningen löses problemet genom ett förfarande för att alstra en krypterings/dekrypteringsnyckel i en första nod, vilken är användbar för säker kommunikation mellan den första noden och en andra nod. Förfarandet enligt den andra aspekten innefattar följande steg att:

skicka en begäran till en central server för att sätta upp en säker kommunikation med den andra noden,

30 motta en första nyckelalstringsfil från den centrala servern i gensvar på denna begäran,

bearbeta den första nyckelalstrande filen,

alstra en första tillfällig datauppsättning,

skicka den första tillfälliga datauppsättningen till den andra noden,

motta en tredje tillfällig datauppsättningen från den andra noden,

jämföra bitarna hos den tredje tillfälliga datauppsättningen med motsvarande bitar i den första tillfälliga datauppsättningen,

5 alstra en första krypteringsnyckel baserad på en bit för bit jämförelse mellan den tredje och den första tillfälliga datauppsättningen genom att behålla värdet hos biten av den första datauppsättningen om den motsvarande biten hos den tredje tillfälliga datauppsättningen är satt till ett första värde och ignorera biten hos den första tillfälliga datauppsättningen om motsvarande bit hos den tredje tillfälliga datauppsättningen är satt till ett andra värde.

10 Enligt en tredje aspekt av den föreliggande uppfinningen löses problemet av ett förfarande för att alstra en krypterings/dekrypteringsnyckel i en andra nod, vilken är användbar för säker kommunikation mellan en första och en andra nod. Enligt denna tredje aspekt innefattar förfarandet följande steg att:

15 motta en andra nyckelalstrande fil från en central server i gensvar på en begäran från den första noden att starta säker kommunikation mellan den första noden och den andra noden,

bearbeta den andra nyckelalstrande filen,
alstra en andra tillfällig datauppsättning,
motta en första tillfällig datauppsättning från den första noden,
20 jämföra bitarna hos den första tillfälliga datauppsättningen med motsvarande bitar hos den andra tillfälliga datauppsättningen,

skapa en ny tredje tillfällig datauppsättning baserad på en bit för bit jämförelse mellan de första och den andra tillfälliga datauppsättningen genom att sätta ett första värde om de jämförda bitarna är lika och ett andra värde i fall de jämförda bitarna är olika,

25 skicka den tredje tillfälliga datauppsättningen till den första noden,
alstra en andra krypteringsnyckel baserad på en bit för bit jämförelse mellan den första och den andra tillfälliga datauppsättningen genom att behålla värdet hos biten i den andra datauppsättningen om motsvarande bit hos den första tillfälliga datauppsättningen är lika och ignorera biten hos den andra tillfälliga datauppsättningen om de jämförda bitarna är olika.
30

Enligt en föredragen utföringsform av den föreliggande uppfinningen innefattar steget att skicka den första och den andra nyckelalstrande filen också skickande av metadata som är bifogat varje nyckelalstringsfil.

I ytterligare en föredragen utföringsform av den föreliggande uppfinningen innefattar metadatat en konstant som kan användas för alstring av både den första och den andra krypteringsnyckeln. Metadatat kan också innefatta information om krypteringsnyckelns längd.

5 I en annan utföringsform kan nyckellängden alstras slumpmässigt inom ett på förhand fastställt intervall.

Enligt en fjärde aspekt av den föreliggande uppfinningen tillhandahålles ett dataprogram som innefattar kod för att utföra stegen i förfarandet när programmet körs på en dator.

10 Enligt en femte aspekt av uppfinningen tillhandahålles en datorprogramprodukt som innefattar programkod lagrad på ett datorläsbart media för att utföra stegen i förfarandet när produkten körs på en dator.

Den stora fördelen med den föreliggande uppfinningen är att nyckeln alstras vid noderna som vill kommunicera med varandra och sålunda finns det inget behov av att distribuera nycklar.

15

Kort beskrivning av ritningarna

Uppfinningen kommer att beskrivas nedan med hänvisning till de bifogade ritningarna, i vilka

20 Fig. 1 är ett flödesschema som visar förfarandet för att alstra en krypteringsnyckel enligt den föreliggande uppfinningen,

Fig. 2 är ett exempel på en nyckelalstringsfil som sänds från den centrala servern till noderna som vill kommunicera,

25 Fig. 3 är ett exempel på en konstant som används för att alstra den första och den andra tillfälliga datauppsättningen,

Fig. 4 är ett exempel på den första tillfälliga datauppsättningen i den första noden A och den andra tillfälliga datauppsättningen vid den andra noden B,

30 Fig. 5 är ett exempel på en matchningsprocess mellan den första och den andra tillfälliga datauppsättningen och alstringen av en krypteringsnyckel för den andra noden B, och

Fig. 6 är ett exempel på alstringen av en krypteringsnyckel för den första noden A.

Detaljerad beskrivning av uppfinningen

Den föreliggande uppfinningen kommer nu att beskrivas i detalj med hjälp av olika utföringsformer därav. Utföringsformerna skall ses som exempel och förklarande för att förstå den föreliggande uppfinningen och inte som begränsande.

5 Fig. 1 visar förfarandet för att alstra en krypteringsnyckel enligt den föreliggande uppfinningen. Det övergripande förfarandet exekveras av två noder A och B som vill sätta upp en säker kommunikation med varandra genom att använda en säker krypterings/dekrypteringsnyckel. Förfarandet exekveras vidare med hjälp av en central server 2. I Fig. 1 visas den första noden A på den vänstra sidan och den andra noden B på den högra sidan, dvs. det steg som utförs av den första noden A visas på den vänstra sidan av den streckade linjen och de steg som utförs av den andra noden B visas på den högra sidan av den streckade linjen. I praktiken kan den första noden A vara en dator vars användare vill påbörja en säker kommunikation med en dator, den andra noden B, hos sin bank. Vilket är uppenbart för fackmannen på området kan både den första noden A och den andra noden B kan vara någon kommunikationsanordning som vill kommunicera med någon annan.

Den centrala servern 2 kan vara någon kommunikationsanordning som är kapabel att motta och skicka data på ett säkert sätt med hjälp av någon typ av säkerhetscertifikat. För att en nod skall kunna använda nyckelalstringsförfarandet enligt den föreliggande uppfinningen måste noden vara auktoriserad att kommunicera med den centrala servern 2. Den centrala servern 2 håller sålunda reda på alla användare som är auktoriserade för att använda nyckelalstringsförfarandet. Såsom nämnts ovan kan kommunikation mellan den centrala servern 2 och noderna eller vice versa göras säker genom att använda någon typ av säkerhetscertifikat. Företrädesvis används ett X509 certifikat eller liknande för den säkra kommunikationen.

Förfarandet för att alstra en krypterings-/dekrypteringsnyckel enligt den föreliggande uppfinningen kommer nu att beskrivas med hjälp av ett exempel. Förfarandet börjar med att en nod, i detta exempel den första noden A, skickar en begäran till den centrala servern 2 för att sätta upp förbindelse med den andra noden B. Den centrala servern 2 kontrollerar först om den första noden A är auktoriserad att kommunicera med den andra noden B och också om den andra noden B är auktoriserad att kommunicera med den centrala servern 2 och den första noden A. Om båda noderna är auktoriserade att starta kommunikation med varandra kommer den centrala servern 2 i gensvar på begäran från den första noden A att skicka en första nyckelalstringsfil till den första noden A och en andra nyckelalstringsfil till den andra noden B.

Fig. 2 visar ett exempel på en nyckelalstringsfil som sänds från den centrala servern till den första noden A och den andra noden B. Filen innefattar en bearbetningsfil som när den exekveras av den första noden A och andra noden B kommer att alstra krypterings/dekrypteringsnyckeln. Eftersom bearbetningen vid den första noden A och den andra noden B skiljer sig åt, vilket kommer att beskrivas nedan, skiljer sig bearbetningsfilen som skickas till den första noden A från den bearbetningsfilen som skickas till den andra noden B. Såsom framgår av Fig. 2 innefattar nyckelalstringsfilen också metadata M1, M2... Mn. Metadata kan innehålla information som används för att alstra krypterings/dekrypteringsnyckeln och samma metadata kommer att skickas både till den första noden A och till den andra noden B. Exempel på metadata är en konstant som används för att alstra nycklarna. Fig. 3 visar ett exempel på en sådan konstant som används för att alstra en första och en andra tillfällig datauppsättning som används under nyckelalstringen. Metadata kan också innefatta en tidmärkning som används för att jämföra om de båda nyckelalstringsfilerna har samma ursprung.

Metadata kan vidare också innefatta information om den nyckellängd som skall användas eller vilka bitar hos nyckeln som skall användas för att alstra nyckeln. Såsom är uppenbart för fackmannen på området så finns det en mängd annat metadata som kan användas för att ytterligare öka säkerheten hos nyckelalstringsprocessen.

När nyckelalstringsfilen har mottagits av den första noden A och den andra noden B, kommer varje nod att påbörja bearbetningen av filen. Nod A kommer först att alstra en första tillfällig datauppsättning och den andra noden B kommer att alstra en andra tillfällig datauppsättning genom att använda värdet på konstanten, såsom visas i Fig. 3. Konstanten innefattar i detta fall fyra binära bitar som hör ihop med en bokstav. Längden hos konstanten kan variera godtyckligt och bitarna som hör ihop därmed kan vara bokstäver, figurer, grekiska symboler etc.

Ett exempel på den första tillfälliga datauppsättningen för den första noden A och den andra tillfälliga datauppsättningen för den andra noden B visas i Fig. 4. De tillfälliga datauppsättningarna alstras genom att använda någon typ av känd pseudoslumptalsgenerator, med användning av sådana pseudoslumpalgoritmer såsom Blum Blum Shub, Fortuna eller Mersenne twister, för att alstra en godtycklig sekvens av i detta fall bokstäverna A-D. Den slumpmässiga sekvensen av bokstäver visas i huvudet av den första och den andra tillfälliga datauppsättningen i Fig.4. För att alstra den tillfälliga datauppsättningen fastställs sekvensen hos bokstäverna pseudoslumpmässigt och därefter kommer det korrekta tillhörande värdet till bokstäverna tilldelas i överensstämmelse med konstanten i Fig. 3. Om tilldelningen resulterar i alstringen av

exempelvis endast nollor eller endast ettor för den tillfälliga datauppsättningen kommer detta resultat att filtreras bort och en ny slumpmässig sekvens kommer att alstras.

Eftersom både den första och den andra tillfälliga datauppsättningen alstras pseudoslumpmässigt kommer de aldrig att vara desamma. Längden hos de tillfälliga datauppsättningarna i detta exempel är endast åtta bitar för att på ett enkelt sätt illustrera den föreliggande uppfinningen i ett exempel. I praktiken är emellertid längden hos de tillfälliga datauppsättningarna typiskt mellan 64 till 2048 bitar. Längden kan vara en del av metadatat såsom nämns ovan och kan sättas godtyckligt av den centrala servern 2 varje gång en ny begäran görs från en nod.

Efter alstringen av den första och den andra tillfälliga datauppsättningen kommer den första noden att skicka den första tillfälliga datauppsättningen till den andra noden B utan något skydd, dvs. publikt.

Den andra noden B kommer att jämföra den första och den andra tillfälliga datauppsättningen med varandra. Resultatet av denna jämförelse kallas Match 1 i tabellen som visas i Fig. 5. Värdet A och värdet B motsvarar den första respektive den andra tillfälliga datauppsättningen. Jämförelsen är en bit för bit jämförelse och resulterar i Sant om värdet för den första och den andra datauppsättningsbiten är lika och Falskt om de är olika. Resultatet, Match 1, av jämförelsen används för att skapa en ny tredje tillfällig datauppsättning, Värde 1, genom att sätta ett första värde om de jämförda bitarna är lika och ett andra värde om de jämförda bitarna är olika. I detta fall används 1 när de jämförda bitarna är lika och 0 används om de jämförda bitarna är olika. Det bör emellertid förstås att det även kan vara tvärtom utan att man avviker från den föreliggande uppfinningen.

Den tredje tillfälliga datauppsättningen skickas sedan publikt från den andra noden B till den första noden A. Den första noden A alstrar sedan en första krypteringsnyckel baserad på en bit för bit jämförelse mellan den tredje och den första tillfälliga datauppsättningen genom att behålla värdet på biten hos den första datauppsättningen om motsvarande bit hos den tredje tillfälliga datauppsättningen är satt till det första värdet och ignorera biten hos den första tillfälliga datauppsättningen om motsvarande bit hos den tredje tillfälliga datauppsättningen är satt till det andra värdet. I detta fall, såsom visas i Fig. 6, motsvarar det första värdet en 1 och det andra värdet en 0. Såsom framgår av Fig. 6 innefattar nyckeln fyra bitar i stället för de ursprungliga åtta bitarna eftersom fyra bitar har ignorerats under alstringen av nyckeln.

Såsom nämnts ovan skickas både den första tillfälliga datauppsättningen och den tredje tillfälliga datauppsättningen publikt. Även om de skulle avlyssnas så finns det inget sätt för en tredje part att alstra en nyckel genom användning av dessa data eftersom värdet hos en 1 i en tredje datauppsättning i verkligheten inte betyder värdet 1, utan endast att den första datauppsättningen och den andra datauppsättningen har samma värde. En 1 i den tredje datauppsättningen kan sålunda faktiskt betyda antingen en 1 eller en 0.

I nod B alstras den andra krypteringsnyckeln baserad på en bit för bit jämförelse mellan den första och den andra tillfälliga datauppsättningen, se Fig. 5, genom att behålla värdet på biten hos den andra datauppsättningen om den motsvarande hos den första tillfälliga datauppsättningen är lika och ignorera biten hos den andra tillfälliga datauppsättningen om de jämförda bitarna är olika. Såsom framgår av figur 5 och 6 är den första och den andra krypteringsnyckeln samma nycklar. Nycklarna kan sedan användas för kryptering/dekryptering av information som sänds mellan den första noden A och den andra noden B. Varje känd krypteringsmetod kan användas tillsammans med nyckeln som alstras av förfarandet enligt den föreliggande uppfinningen. Den föreliggande uppfinningen är sålunda inte inriktad på hur krypteringen/dekrypteringen görs men är i stället inriktad på hur krypteringsnycklarna alstras. Den altrade nyckeln kommer att vara giltig så länge som kommunikationen pågår mellan den första och den andra noden. När nyckeln har alstrats av den första noden A och den andra noden B, kommer nyckelalstringsfilerna som mottas av den centrala servern att raderas i respektive nod.

Det övergripande förfarandet för den föreliggande uppfinningen har nu beskrivits i detalj. Den föreliggande uppfinningen hänför sig emellertid också till ett förfarande för att alstra en kryptering/dekrypteringsnyckel vid den första noden A. Detta förfarande är en del av det övergripande förfarandet som beskrivits ovan och kommer därför endast att beskrivas kort. Förfarandet som exekveras av den första noden startar med att en begäran skickas till den centrala servern 2 för att sätta upp en säker kommunikation med den andra noden B. Den första noden mottar sedan den första nyckelalstringsfilen från den centrala servern och börjar bearbeta den. Detta kommer att alstra den första tillfälliga datauppsättningen, som såsom nämnts ovan skickas till den andra noden B.

Den första noden A kommer sedan att motta den tredje tillfälliga datauppsättningen från den andra noden B och jämföra bitarna hos den tredje tillfälliga datauppsättningen med motsvarande bitar hos den första tillfälliga datauppsättningen. Den första

noden A kommer att alstra den första krypteringsnyckeln baserad på en bit för bit jämförelse mellan den tredje och den första tillfälliga datauppsättningen genom att behålla värdet på biten hos den första datauppsättningen om motsvarande bit hos den tredje tillfälliga datauppsättningen är satt till det första värdet och ignorera biten hos den första tillfälliga datauppsättningen om motsvarande bit hos den tredje tillfälliga datauppsättningen är satt till det andra värdet.

Också den andra noden B kommer att exekvera en del av det övergripande förfarandet, som nu kommer att beskrivas kort. Förfarandet för att alstra en krypterings-/dekrypteringsnyckel i den andra noden B börjar med att den andra noden B mottar den andra nyckelalstringsfilen från den centrala servern 2 och påbörjar bearbetning därav. Detta kommer att alstra den andra tillfälliga datauppsättningen. Den andra noden B kommer därefter att motta den första tillfälliga datauppsättningen från den första noden A och jämföra bitarna hos den första tillfälliga datauppsättningen med motsvarande bitar hos den andra tillfälliga datauppsättningen. Därefter kommer den andra noden B att skapa en ny tredje tillfällig datauppsättning baserad på en bit för bit jämförelse mellan den första och den andra tillfälliga datauppsättningen genom att sätta det första värdet om de jämförda bitarna är lika och det andra värdet om de jämförda bitarna är olika. Den tredje tillfälliga datauppsättningen skickas sedan till den första noden A.

Den andra noden B alstrar sedan den andra krypteringsnyckeln baserad på en bit för bit jämförelse mellan den första och den andra tillfälliga datauppsättningen genom att behålla värdet för biten hos den andra datauppsättningen om motsvarande bit hos den första tillfälliga datauppsättningen är lika och ignorera biten hos den andra tillfälliga datauppsättningen om den jämförda biten är olika.

Med förfarandet som beskrivits ovan är det sålunda möjligt att på ett enkelt och säkert sätt alstra krypteringsnycklar där de används, dvs. vid noderna. Detta är särskilt fördelaktigt eftersom behovet att distribuera nycklar inte längre finns. Nyckeln är av engångstyp och kommer att vara giltig endast för en kommunikationssession och så länge som den är aktiv. Nycklarna alstras vidare i två oberoende processer vid två separata noder.

Även om det anses att det ovan beskrivna förfarandet är mycket säkert så kan säkerheten höjas ytterligare genom att använda metadata som bifogas nyckelalstringsfilen. Till exempel kan metadata fastställa att endast var tredje eller varannan bit av resultatet i nyckelalstringsprocessen skall användas som en nyckel. På liknande sätt kan metadata användas också för att fastställa att endast var tredje eller varannan bit skall

läsas när den första noden A och andra noden B kommunicerar med varandra under nyckelalstringsprocessen.

- Det skall förstås att även om uppfinningen har beskrivits med hänvisning till föredragna utföringsformer så är inte uppfinningen begränsad till detta. Det finns många
- 5 olika utföringsformer och varianter som likväl ligger inom uppfinningens omfattning som definieras bäst av de bifogade patentkraven.

PATENTKRAV

1 Ett förfarande för att alstra en krypterings-/dekrypteringsnyckel, som vilken är användbar för säker kommunikation mellan en första nod (A) och en andra nod (B), varvid förfarandet innefattar följande steg:

5 skicka en begäran från den första noden (A) till en central server (2) för att sätta upp en förbindelse med den andra noden (B),

skicka en första nyckelalstringsfil från den centrala servern (2) till den första noden (A) och en andra nyckelalstringsfil till den andra noden (B) i gensvar på begäran från den första noden (A),

10 påbörja bearbetandet av den första nyckelalstringsfilen i den första noden (A) och den andra nyckelalstringsfilen i den andra noden (B),

alstra en första tillfällig datauppsättning vid den första noden (A) och en andra tillfällig datauppsättning vid den andra noden (B),

15 skicka den första tillfälliga datauppsättningen från den första noden (A) till den andra noden (B),

jämföra bitarna i den första tillfälliga datauppsättningen med motsvarande bitar i den andra tillfälliga datauppsättningen,

20 skapa en ny tredje tillfällig datauppsättning baserad på en bit för bit jämförelse mellan den första och den andra tillfälliga datauppsättningen genom att sätta ett första värde om de jämförda bitarna är lika och ett andra värde om de jämförda bitarna är olika,

skicka den tredje tillfälliga datauppsättningen från den andra noden (B) till den första noden (A),

25 jämföra bitarna hos den tredje tillfälliga datauppsättningen med motsvarande bitar hos den första tillfälliga datauppsättningen,

30 alstra en första krypteringsnyckel baserad på en bit för bit jämförelse mellan den tredje och den första tillfälliga datauppsättningen genom att behålla värdet hos biten hos den första datauppsättningen om motsvarande bit hos den tredje tillfälliga datauppsättningen är satt till det första värdet och ignorera biten för den första tillfälliga datauppsättningen om motsvarande bit hos den tredje tillfälliga datauppsättningen är satt till det andra värdet,

alstra en andra krypteringsnyckel baserad på en bit för bit jämförelse mellan den första och den andra tillfälliga datauppsättningen genom att behålla värdet hos biten hos den andra datauppsättningen om motsvarande bit hos den första tillfälliga datauppsättningen är lika och ignorera biten hos den andra tillfälliga datauppsättningen om de

jämförda bitarna är olika, varvid den första och den andra krypteringsnyckeln är desamma.

2. Ett förfarande enligt patentkrav 1, i vilket steget att skicka den första nyckelalstringsfilen till den första noden (A) och den andra nyckelalstringsfilen till den andra noden (B) också innefattar skickandet av metadata bifogat i respektive nyckelalstringsfil.

3. Ett förfarande enligt patentkrav 2, i vilket metadatat innefattar en konstant som används för att alstra både den första och den andra krypteringsnyckeln.

4. Ett förfarande enligt patentkrav 2 eller 3, i vilket metadatat innefattar information om krypteringsnyckelns längd.

5. Ett förfarande enligt patentkrav 4, ytterligare innefattandet steget att inom ett på förhand fastställt intervall slumpmässigt alstra krypteringsnyckelns längd.

6. Ett förfarande för att alstra en krypterings-/dekrypteringsnyckel i en första nod (A), vilken är användbar för säker kommunikation mellan den första noden (A) och en andra nod (B), varvid förfarandet innefattar stegen att

skicka en begäran till en central server (2) för att sätta upp en förbindelse med den andra noden (B),

motta en första nyckelalstringsfil från den centrala servern (2) i gensvar på begäran,

bearbeta den första nyckelalstringsfilen,

alstra en första tillfällig datauppsättning,

skicka den första tillfälliga datauppsättningen till den andra noden (B),

motta en tredje tillfällig datauppsättning från den andra noden (B),

jämföra bitarna hos den tredje tillfälliga datauppsättningen med motsvarande bitar hos den första tillfälliga datauppsättningen,

alstra en första krypteringsnyckel baserad på en bit för bit jämförelse mellan den tredje och den första tillfälliga datauppsättningen genom att behålla värdet i den första datauppsättningen om motsvarande bit i den tredje tillfälliga datauppsättningen är satt till ett första värde och ignorera biten i den första tillfälliga datauppsättningen om motsvarande bit i den tredje tillfälliga datauppsättningen är satt till ett andra värde.

7. Ett förfarande enligt patentkrav 6, i vilket steget att motta den första nyckelalstringsfilen också innefattar mottagandet av metadata bifogat i filen.

8. Ett förfarande enligt patentkrav 7, i vilket metadatat innefattar en konstant som används för alstring av den första krypteringsnyckeln.

9. Ett förfarande enligt patentkrav 7 eller 8, i vilket metadatat innefattar information om krypteringsnyckelns längd.

10. Ett förfarande för att alstra en krypterings-/dekrypteringsnyckel i en andra nod (B), ~~som~~ vilken är användbar för säker kommunikation mellan en första nod (A) och den andra noden (B), varvid förfarandet innefattar stegen:

att motta en andra nyckelalstringsfil från en central server (2) i gensvar på en begäran från den första noden (A) för att påbörja säker kommunikation mellan den första noden (A) och den andra noden (B),

bearbeta den andra nyckelalstringsfilen,

alstra en andra tillfällig datauppsättning,

motta en första tillfällig datauppsättning från den första noden (A),

jämföra bitarna hos den första tillfälliga datauppsättningen med motsvarande bitar hos den andra tillfälliga datauppsättningen,

skapa en ny tredje tillfällig datauppsättning baserad på en bit för bit jämförelse mellan den första och den andra tillfälliga datauppsättningen genom att sätta ett första värde om de jämförda bitarna är lika och ett andra värde om de jämförda bitarna är olika,

skicka den tredje tillfälliga datauppsättningen till den första noden (A),

alstra en andra krypteringsnyckel baserad på en bit för bit jämförelse mellan den första och den andra tillfälliga datauppsättningen genom att behålla värdet hos biten för den andra datauppsättningen om motsvarande bit för den första tillfälliga datauppsättningen är lika och ignorera biten hos den andra tillfälliga datauppsättningen om de jämförda bitarna är olika.

11. Ett förfarande enligt patentkrav 10, i vilket steget att motta den andra nyckelalstringsfilen också innefattar mottagandet av metadata bifogat i filen.

12. Ett förfarande enligt patentkrav 11, i vilket metadatat innefattar en konstant som används för att alstra den andra krypteringsnyckeln.

13. Ett förfarande enligt patentkrav ~~10-11~~ eller ~~11-12~~, i vilket metadatat innefattar information om krypteringsnyckelns längd.

14. Ett datorprogram innefattande kod för att utföra stegen enligt något av patentkraven 1 - 13, när programmet körs på en dator.

15. En datorprogramprodukt innefattande programkod lagrad i ett datorläsbart media för att utföra förfarandet enligt något av patentkraven 1 - 13, när produkten körs på en dator.

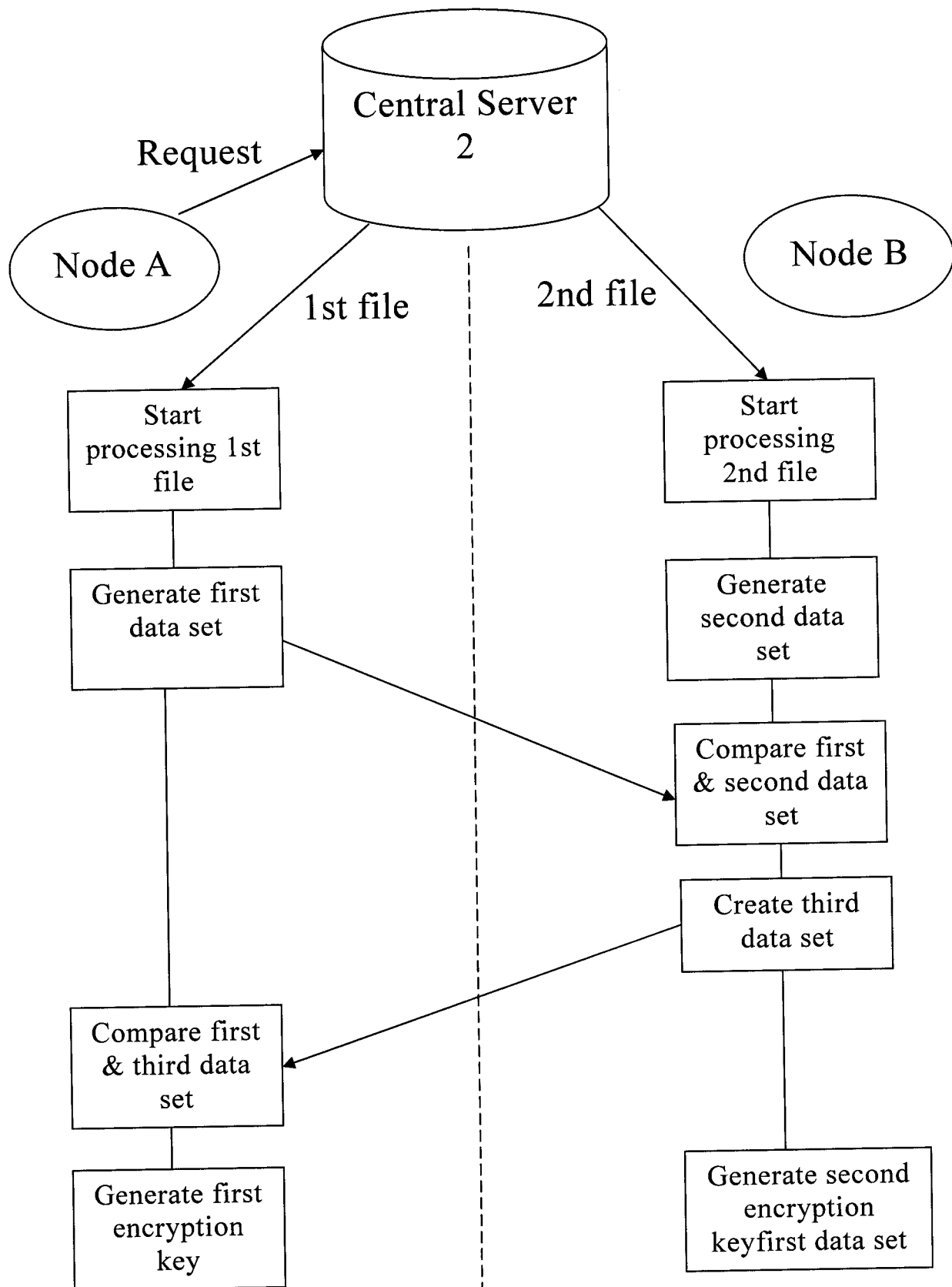


Fig. 1

Process file	M1	M2	Mn
--------------	----	----	----

Fig. 2

A	B	C	D
1	0	1	0

Fig. 3

D	C	A	A	C	B	D	B
0	1	1	1	1	0	0	0

Node A

A	C	A	B	D	B	D	C
1	1	1	0	0	0	0	1

Node B

Fig. 4

Value A	0	1	1	1	1	0	0	0
Value B	1	1	1	0	0	0	0	1
Match 1	F	T	T	F	F	T	T	F
Value 1	0	1	1	0	0	1	1	0
Key B	-	1	1	-	-	0	0	-

Fig. 5

Value A	0	1	1	1	1	0	0	0
Value 1	0	1	1	0	0	1	1	0
Key A	-	1	1	-	-	0	0	-

Fig. 6