
بسم الله الرحمن الرحیم

دانشگده فنی و مهندسی

گروه کامپیوتر

پایان‌نامه جهت اخذ درجه کارشناسی ارشد رشته مهندسی فناوری اطلاعات– گرایش شبکه‌های کامپیوتری

موضوع:

پروتکل‌های مدیریت کلید در شبکه‌های بی‌سیم برای ارتباطات گروهی

استاد راهنما:

دکتر جمشید باقرزاده

تنظیم و نگارش:

عبداله جباری

شهریور ۱۳۹۱

تشکر و قدردانی

پروردگارا، ای هستی بخش وجود، مرا به نعمات بیکرانت توان شکر نیست. خداوندا تو را سپاس می‌گویم که در لحظه لحظه زندگی یاورم بودی و ازدریچه لطف و رحمت خود بر من منت نهاده، وجود تشنه‌ام را جرعه‌ای از علم و معرفت حیات بخشیدی.

اینک که به لطف پروردگار مهربان، این تحقیق به پایان رسیده است، بر خود لازم می‌دانم از تمامی اساتید محترمی که در طول تحصیل از محضر ایشان کسب فیض نموده‌ام و همچنین ازسایر بزرگواران و سرورانی که مرا در انجام این تحقیق یاری نموده اند، تشکر و قدردانی کنم.

با تشکر و قدردانی فراوان از استاد راهنمای گرامی، جناب آقای دکتر جمشید باقرزاده که همواره با روی گشاده مرا پذیرا بودند و با دریای صبر، شخصیت والا و رهنمودهای ارزشمند علمی و اخلاقی خویش، راهنمایم بودند.

با سپاس فراوان از آقای دکتر وحید سلوک (داور خارجی)، و آقای دکتر صالح یوسفی (داور داخلی) که در نهایت لطف، پایان نامه را مطالعه و نظرات اصلاحی خود را ابراز نمودند.

همچنین از کلیه عزیزانی که همواره در مسیر علم و دانش پشتیبان و مشوق من بودند بخصوص پدر و مادر دلسوزم که تمامی زندگی و آرزوهای خودشان را خالصانه در راه تحصیل علم و دانش فرزندانشان گذاشته و می گذارند تشکر و قدردانی می‌کنم.

از مرکز تحقیقات مخابرات ایران که این پایان‌نامه را تحت قرارداد شماره ۵۰۰/۱۹۲۴۶/ت مورخه ۹۰/۱۲/۲۸ بین آن مرکز و دانشگاه ارومیه مورد حمایت مالی آن مرکز قرار داده است، قدردانی می‌کنم.

چکیده

ارتباطات چند پخشی یک ابزار موثر برای توزیع داده بین اعضای یک گروه می‌باشد. از میان مشکلات امنیتی که در ارتباطات گروهی وجود دارد مدیریت کلید نقش مهمی دارد. شبکه‌های بی‌سیم مخصوصا شبکه‌های بی‌سیم سیار به خاطر خصوصیاتی مانند رسانه دسترسی مشترک، عدم وجود مدیریت مرکزی و ساختار پویا بیشتر در مقابل حملات امنیتی آسیب‌پذیر هستند، بنابراین به مکانیزمهای امنیتی برای حل این مشکل نیاز داریم. پروتکل‌های توافق کلید گروه به یک مجموعه از کاربران اجازه می‌دهند تا بر روی یک شبکه عمومی به یک کلید مشترک برای گروه به توافق برسند بطوریکه کلید حاصل شده حاوی سهم هرکاربر می‌باشد و کلید توافق شده می‌تواند در ارتباطات گروهی امن به کار رود. به همین جهت کارایی این پروتکل‌ها از نظر امنیت از اهمیت خاصی برخودار است. از طرف دیگر، برای امنیت بیشتر، گمنامی کاربر در زمان توافق کلید موضوع مهمی به شمار می‌رود. به همین جهت برای بهبود امنیت ابتدا روشی جدید و امن برای توافق کلید گروه با استفاده از نگاشت آشوب چبیشف ارایه می‌شود که به کاربران اجازه می‌دهد با حفظ امنیت گروه، به گروه اضافه شوند و یا گروه را ترک کنند. برای حفظ گمنامی در زمان توافق کلید، با استفاده از نگاشت آشوب چبیشف، ابتدا کارهای انجام شده در این زمینه را تحلیل کرده و ضعف‌های آنها را بیان می‌کنیم، سپس یک پروتکل بهبود یافته براساس نگاشت آشوب پیشنهاد می‌کنیم. پروتکل پیشنهاد شده این مشکلات را حل می‌کند و به کاربر اجازه می‌دهد به صورت گمنام به یک کلید توافقی دست یابد.

از طرف دیگر کارایی پروتکل‌های توافق کلید از نظر سربار محاسباتی و ارتباطی برای حالتی که شبکه خیلی پویا و یا گره‌های شبکه منابع محدودی دارند موضوع مهمی می‌باشد. بنابراین برای بهبود کارایی از نظر سربار محاسباتی و ارتباطی یک پروتکل توافق کلید گروه پیشنهاد می‌کنیم بطوریکه گره‌ها بتوانند کلید گروه را با سربار محاسباتی و ارتباطی کمتری پیدا کنند.

کلمات کلیدی: امنیت شبکه، توافق کلید گروه ، نگاشت آشوب چبیشف، مدیریت کلید گروه، گمنامی

فهرست مطالب

عنوان **صفحه**

فهرست جدول‌ها

عنوان **صفحه**

فهرست شکل‌ها

عنوان **صفحه**

فصل ۱ مقدمه

۱-۱ پیشگفتار

ارتباطات چند پخشی[1] مانند آنچه که در [۱] تعریف شده یک ابزار موثر برای توزیع داده بین اعضای یک گروه می‌باشد[۲]. ارتباطات گروهی کاربردهای[2] زیادی دارد، مانند بروز رسانی فایل یا نرم افزار، ارسال دستور، ارسال صدا و ویدیو[3] و کاربردهای نظامی[۳].

ارتباطهای چندپخشی نیاز به مکانیزم‌هایی برای کنترل دسترسی به داده‌های ارسال شده ومحافظت ارتباطات گروه از اعضای غیر مجاز[4] دارد[۲]. از میان مشکلات امنیتی که در ارتباطات گروهی وجود دارد مدیریت کلید از اهمیت خاصی برخودار است. پروتکل های مدیریت کلید، هسته‌ی[5] ارتباطات امن می-باشد[۵,۴]. پروتکل‌های مدیریت کلید مسئول برپا[6] کردن کانال امن بین گره‌ها می‌باشند[۶]. برای اینکه اطلاعات بصورت امن بین اعضای گروه(گره‌ها) چندپخشی شود لازم است که اعضای گروه یک کلید را به صورت امن بین خود به اشتراک گذاشته باشند. هربسته اطلاعاتی باید قبل از ارسال با کلید گروه رمز شود و تنها گره‌های مجاز اعضای گروه که کلید گروه را در اختیار دارند می‌توانند بسته اطلاعاتی را رمزگشایی کنند، کاربران غیرمجاز احتمالا بسته اطلاعاتی را دریافت می‌کنند ولی بدون در اختیار داشتن کلید گروه نمی‌توانند بسته اطلاعاتی را رمز گشایی کنند، بنابراین ارتباطات بین اعضای گروه امن باقی می‌ماند[۳].

اعضای گروه ممکن است تغییر کنند. زمانی که عضو جدیدی وارد گروه شود برای اینکه اطلاعات قبلی امن بماند و عضو جدید نتواند به اطلاعات قبلی دست یابد باید کلید گروه عوض شود و همچنین اگر عضوی گروه را ترک کند نباید به اطلاعاتی که در آینده بین اعضای گروه منتقل می‌شود دسترسی داشته باشد و در این موقع نیز باید کلید گروه عوض شود. بنابراین برای ارتباط امن بین اعضای گروه نیاز به

[1] Multicast Communication
[2] Applications
[3] Video-audio transmission
[4] Illegitimate
[5] core
[6] Establish

مکانیزم مدیریت کلید وجود دارد تا که اعضای گروه با آن بتوانند به نحوی کلیدی را تولید و بین خود به اشتراک بگذارند و درصورت لزوم این کلید را عوض[۱] کنند.

پروتکل‌های مدیریت کلید مسئول برپا کردن و نگهداری از کلید گروه می‌باشند. این کلید محرمانه گروه باید به صورت امن و کارا بین تمامی اعضای گروه توزیع شود[۷].

پروتکل‌های مدیریت کلید را می‌توان به سه دسته طبقه بندی کرد: متمرکز[۲]، غیر متمرکز[۳] و توزیع شده[۴] [۸].

در پروتکل‌های مدیریت کلید به صورت متمرکز یک سرویس دهنده کلید گروه[۵] (KS) وجود دارد که مسئولیت تولید و توزیع و به‌روز رسانی کلید گروه را به عهده دارد. پروتکل‌های مختلفی برای مدیریت کلید بصورت متمرکز تعریف شده که LKH[۶] و OFT[۷] نمونه‌هایی از این پروتکل‌ها می‌باشند[۱۱,۱۰,۹]. در پروتکل LKH یک درخت منطقی کلید توسط KS نگهداری می‌شود که ریشه این درخت نشان دهنده‌ی کلید گروه است که برای رمز کردن داده‌ها در ارتباطات گروه استفاده می‌شود. این کلید بین همه گره‌ها به اشتراک گذاشته شده است. برگ‌های این درخت نشان دهنده‌ی کلید محرمانه بین هر گره و KS می-باشد و کلیدهای وسطی نشان دهنده KEK ها (کلیدی که برای رمز کردن کلید گروه استفاده می‌شود) می‌باشد که برای توزیع کلید ریشه استفاده می‌شوند و هر گره تمام کلیدها در مسیر مربوط به خود از برگ تا ریشه درخت را در اختیار دارد و زمانی که گرهی وارد گروه شود یا گروه را ترک کند تمام کلیدهای مربوط به آن از برگ تا ریشه باید تغییر کند[۱۰]. در شبکه‌های بی‌سیم با تعداد گره‌های زیاد و پویا[۸] بخاطر محدودیت منابع از جمله پهنای باند و قدرت محاسباتی گره‌ها، KS گلوگاه[۹] می‌شود و اگر KS از کار بیافتد کل ارتباط امن گروه از کار خواهد افتاد[۱۲].

در پروتکل‌های غیر متمرکز کل گروه به زیرگروه‌هایی تقسیم می‌شود و برای کل گروه یک کلید وجود دارد و بین عضوهای هر زیرگروه نیز یک کلید مشترک جداگانه وجود دارد و برای کل گروه یک (KS)

---

[1] Update
[2] Centralized
[3] Decentralized
[4] Distributed
[5] Group Key Server
[6] Logical Key Hierarchy
[7] One-way hash Function Tree
[8] Highly Dynamic
[9] Bottleneck

وجود دارد که عمل مدیریت کلید را برای کل گروه انجام می‌دهد و برای هر زیرگروه هم یک سرور کلید زیرگروه[۱] (SGK) وجود دارد که عمل مدیریت کلید برای زیرگروه مورد نظر را انجام می‌دهد. بعنوان مثال IGKMP[۲] و SMKD[۳] دو نمونه از پروتکل‌های غیرمتمرکز می‌باشند[۱۴,۱۳,۳]. حالت غیرمتمرکز رهیافت رهیافت مفیدی برای مقابله با مشکل مقیاس‌پذیری[۴] برای مدیریت کلید گروه در یک محدوده وسیع فراهم می‌کند که درآن کل گروه را به زیرگروها تقسیم می‌کند و عمل مدیریت در هر زیرگروه را بصورت جداگانه انجام می‌دهد. بنابراین این روش برای شبکه‌های بی‌سیم با وسعت گسترده مانند شبکه‌های سلولی، وایمکس و سیستم های 4G مفید می‌باشد[۱۲].

برخلاف دو روش قبل در حالت توزیع‌شده تعداد زیادی از اعضای گروه در تولید و توزیع کلید مشارکت دارند. بعنوان مثال TGDH[۵] ، BD[۶] و GDH[۷] نمونه‌هایی از پروتکل‌های مدیریت کلید به صورت توزیع شده هستند[۱۷,۱۶,۱۵]. در فصل سوم مثال‌هایی از پروتکل‌های مدیریت کلید توزیع شده آمده است.

در روش‌های‌توزیع شده مشکل از کارافتادن سرور[۸] وجود ندارد ولی لازم است که گره‌ها محاسبات زیادی انجام دهند که ممکن است در یک گروه بزرگ دستیابی به یک کلید مشترک زمان‌بر باشد، اما برای شبکه‌هایی مانند MANET بهترین گزینه است[۳].

با توجه به مطالب مطرح شده می‌توان دریافت که مطالعه و بررسی پروتکل‌های مدیریت کلید گروه هم از نظر کارایی و هم ار نظر امنیتی از اهمیت زیادی برخوردار است و در میان این پروتکل‌ها، پروتکل-های مدیریت کلید توزیع شده، جایگاه ویژه‌ای دارد. بنابراین در این پایان‌نامه ما فقط پروتکل‌های مدیریت کلید توزیع شده را مد نظر قرار می‌دهیم.

یک سیستم آشوب بوسیله‌ی وابستگی حساس به شرایط مقدار اولیه و شبه تصادفی و ergodicity مشخص می‌شود[۵۴]. این خصوصیات شرایط خوبی را برای پخش شدگی[۹] و اغتشاش[۱] که برای

---

[1] Sub Group Key Server
[2] Intra Domain Group Key Management Protocol
[3] Scalable Multicast Key Distribution
[4] Scalability
[5] Tree – Based Diffie – Hellman
[6] Burmester Desmedt
[7] Group Diffie Hellman
[8] Single-Point Error
[9] Diffusion

رمزنگاری لازم هستند فراهم می‌کنند[۵۵]. به همین جهت امروزه این نگاشت مورد توجه محققان در زمینه رمزنگاری قرار گرفته است و مزایای این نگاشت شروعی برای پیشنهادات جدید در حوزه رمزنگاری شده است.

در این پایان‌نامه ما فرض می‌کنیم که انتقال داده در شبکه و بین گره‌ها قابل اعتماد[۲] است به عبارت دیگر فرض می‌کنیم که بسته‌ها در شبکه گم نمی‌شوند و فرض می‌شود که تحویل پیام‌ها[۳] به صورت مرتب[۴] می‌باشد.

۱–۲ اهداف پایان‌نامه

هدف این پایان‌نامه ارائه و بهبود پروتکل‌های توافق کلید چه از نظر امنیتی و چه از نظر هزینه محاسباتی و ارتباطی می‌باشد. در زمینه بهبود امنیت دو پروتکل بررسی می‌شود. پروتکلی که امکان توافق کلید گروه را فراهم کند بطوریکه نسبت به روشهای قبلی ارائه شده امن‌تر باشد. برای این منظور از نگاشت آشوب چیبیشف استفاده شده است و با استفاده از این نگاشت یک روش جدید برای توافق کلید گروه ارائه می‌شود. قسمت بعدی، مطالعه و بررسی پروتکل‌های توافق کلید براساس نگاشت آشوب چبیشف می‌باشد بطوریکه گمنامی کاربر را در موقع توافق کلید فراهم می‌کنند. در این مورد ضمن بررسی پروتکل‌های ارائه شده، مشکلات این پروتکل‌ها بیان می‌شود و سعی می‌شود که یکی از این پروتکل‌ها بهبود داده شود تا این مشکلات حل شود.

در بهبود کارایی از نظر سربار محاسباتی و ارتباطی، سعی می‌شود تا یک پروتکل توافق کلید گروه برای گره‌هایی که امکانات محدودی دارند ارائه شود بطوریکه هم از نظر تعداد پیامهای مبادله شده کارا باشد و هم اینکه گره‌ها محاسبات کمتری را برای رسیدن به کلید گروه انجام دهند.

۱–۳ ساختار پایان‌نامه

در ادامه و در فصل ۲ ابتدا مفاهیم مربوط به رمزنگاری و تعاریف مربوطه آورده شده است. در فصل ۳ مروری بر پروتکل‌های توافق کلید گروه بیان شده است در فصل ۴ پروتکل‌های توافق کلید ارایه شده با

---

[1] Confusion
[2] Reliable
[3] Delivery
[4] Ordered

استفاده از نگاشت آشوب با قابلیت گمنامی کاربر در زمان توافق کلید، بیان شده است و سپس تحلیل هر یک از این پروتکل‌ها آورده شده است. در قسمت اول فصل ۵ ابتدا با استفاده از نگاشت آشوب چبیشف یک پروتکل توافق کلید گروه ارایه شده است. در قسمت دوم این فصل یک پروتکل بهبود یافته برای توافق کلید با استفاده از نگاشت آشوب با قابلیت گمنامی کاربر در زمان توافق کلید، پیشنهاد شده است. در قسمت سوم این فصل یک پروتکل توافق کلید گروه کارا برای شبکه‌های پویا و یا شبکه‌ها با گره‌هایی دارای منابع محدود پیشنهاد شده است. در نهایت فصل ۶ به نتیجه‌گیری اختصاص یافته است.

فصل ۲ مفاهیم پایه

در این فصل مفاهیم مربوط به رمزنگاری و تعاریف مربوطه که در پروتکل‌های توافق کلید وجود دارد بیان می‌شوند.

۲–۱ مساله لگاریتم گسسته[1]

مسأله لگاریتم گسسته به صورت زیر است.

برای گروه دوری[2] G از مرتبه N و مولد e و $\varphi \epsilon G$ داده شده، عدد صحیح x با شرط $0 \leq x \leq N-1$ را طوری پیدا کنید که $e^x = \varphi$.

تاکنون هیچ الگوریتمی با زمان چند جمله‌ای برای حل مساله لگاریتم گسسته پیشنهاد نشده است و امنیت بسیاری از روش های رمزنگاری بر پایه حل مساله لگاریتم گسسته می‌باشد.

۲–۲ مساله دیفی– هلمن[3]

برای گروه دوری G و مولد e با داشتن مقادیر e^a و e^b نمی‌توان مقدار e^{ab} را محاسبه کرد. مساله دیفی-هلمن با مساله لگاریتم گسسته ارتباط نزدیک دارد پیچیدگی حل مساله دیفی-هلمن کوچکتر یا مساوی با پیچیدگی حل مساله لگاریتم گسسته می‌باشد. یعنی اگر مساله لگاریتم گسسته حل شود مساله دیفی-هلمن نیز حل خواهد شد ولی تا حالا اثبات نشده که اگر مساله دیفی-هلمن حل شود آیا مساله لگاریتم گسسته هم حل خواهد شد یا خیر.

۲–۳ مساله تجزیه اعداد صحیح

عدد صحیح n داده شده است آن را به عوامل اول تجزیه کنید.

حل مساله فوق برای زمانی که n عدد بزرگی باشد از نظر محاسباتی در زمان منطقی غیر ممکن است.

---

[1] The discrete logarithm problem

[2] Cyclic Group

[3] Diffie-Hellman problem

۲–۴ تبادل کلید دیفی هلمن[1]

کاربر A و کاربر B با استفاده از تبادل کلید دو قسمتی دیفی هلمن می‌توانند یک کلید مشترک امن محرمانه K را تولید کنند بطوری که توسط هر دوی آنها مشترک باشد[۱۸].

فرض کنید که p عدد اول بزرگ و e یک مولد از GF(p) باشد و زوج (p, e) برای هر دو کاربر معلوم باشد. در این صورت با استفاده از گام‌های زیر گره‌های A و B می‌توانند به یک کلید مشترک محرمانه دست یابند.

گام(۱): کاربر A و B به ترتیب اعداد صحیح تصادفی a و b را تولید می‌کنند که در آن $0 < a < p-1$ و $0 < b < p-1$ می‌باشد.

گام(۲): کاربر A و B به ترتیب مقایر $e^{a} \bmod p$ و $e^{b} \bmod p$ را محاسبه می‌کنند و نتیجه را باهم مبادله می‌کنند.

گام(۳): کاربرA می‌تواند کلید محرمانه را بصورت زیر محاسبه می‌کند.

$$K = (e^{b})^{a} \bmod p = e^{ba} \bmod p$$

و کاربر B کلید محرمانه را بصورت زیر محاسبه می‌کند.

$$K = (e^{a})^{b} \bmod p = e^{ab} \bmod p$$

به این طریق هر دو کاربر می‌توانند بروی یک شبکه عمومی، به یک کلید مشترک محرمانه دست یابند.

۲–۵ سیستم رمز RSA

الگوریتم سیستم رمز RSA یک سیستم رمز همگانی است که بر پایه سختی مساله تجریه اعداد بزرگ می‌باشد. تولید کلید و رمزنگاری بر اساس سیستم رمز RSA به صورت زیر می‌باشد.

۲–۵–۱ الگوریتم تولید کلید برای سیستم رمز RSA

در این سیستم رمز هر کاربر یک کلید عمومی همگانی دارد و یک کلید خصوصی متناظر با کلید عمومی، مراحل تولید این کلید و استفاده آن برای دو کاربر A و B بصورت زیر می‌باشد.

گام(۱): ابتدا کاربر A دو عدد اول بزرگ متمایز را بصورت تصادفی انتخاب می‌کند.

[1] Diff-Hellman Key exchange

گام(۲): مقدار $n = p \times q$ و $\emptyset(n) = (p-1) \times (q-1)$ را محاسبه می‌کند که در آن $\emptyset(n)$ تابع فی اویلر می‌باشد.

گام(۳): عدد تصادفی s، $1 < s < \emptyset(n)$ را طوری انتخاب می‌کند که درآن $gcd\,(s, \emptyset(n)) = 1$.

گام(۴): مقدار f ، $1 < f < \emptyset(n)$ را طوری پیدا می‌کند که در آن $sf \equiv 1\ mod\ \emptyset(n)$.

گام(۵): حال A زوج (n,s) را بعنوان کلید عمومی خود اعلام می‌کند.

۲-۵-۲ الگوریتم سیستم رمز RSA

فرض کنیم که کاربر B بخواهد پیام m را بصورت امن برای کاربر A بفرستد برای این کار ابتدا کاربر B پیام را رمز می‌کند و به کاربر A می‌فرستد و کاربر A پیام را رمزگشایی می‌کند و پیام m را استخراج می-کند.

۲-۵-۳ رمزگذاری پیام

برای رمزگذاری، کاربر B گام‌های زیر را انجام می‌دهد.

گام(۱): ابتدا کاربر B کلید عمومی و معتبر کاربر A را بدست می‌آورد.

گام(۲): پیام m را به یک عدد صحیح در بازه $[0, n-1]$ تبدیل می‌کند.

گام(۳): مقدار $C = m^s\ mod\ n$ را محاسبه می‌کند.

گام(۴): مقدار رمز C را به کاربر A ارسال می‌کند.

۲-۵-۴ رمزگشایی پیام

حال کاربر A می‌تواند پیام رمز C را بصورت زیر رمزگشایی کند و پیام m را بدست آورد.

$m = C^f\ mod\ n$

که در آن f کلید خصوصی کاربر A می‌باشد.

۲-۶ نگاشت آشوب چبیشف

چند جمله‌ای چبیشف بصورت مقابل می‌باشد.

$$T_r(x) = 2xT_{r-1}(x) - T_{r-2}(x)\ Where\ r \geq 2,\quad T_0(x) = 1\ and\ T_1 = x \qquad (۱)$$

که در آن r یک عدد صحیح، نشان دهنده درجه چندجمله‌ای و x نشان دهنده متغیر تصادفی که مقداری را از بازه [-1,+1] می‌گیرد.

یکی از مهمترین خصوصیات چندجمله‌ای چبیشف خصوصیت نیم گروه[1] آن می‌باشد که

$$T_r(T_s(x)) = T_{rs}(x) \qquad (۲)$$

نتیجه این خصوصیت این است که ترکیب چندجمله‌ای‌های چبیشف جابجایی پذیر است. یعنی:

$$T_r(T_s(x)) = T_s(T_r(x)) \qquad (۳)$$

به منظور بهبود خصوصیت نگاشت آشوب چبیشف، Zang [۱۹] اثبات کرد که خصوصیت نیم گروه برای حالتی که x در بازه (∞+,∞-) می‌باشد، نیز برقرار است.

۲-۷ توافق کلید با استفاده از نگاشت آشوب چبیشف

با توجه به خصوصیت (۳) می‌توان از این خصوصیت همانند روش دیفی-هلمن برای ایجاد کلید مشترک بین دو گره استفاده کرد. برای این کار یکی از گره‌ها که شروع کننده ارتباط می‌باشد مثلا گره A اعداد تصادفی بزرگ r، x و عدد اول بزرگ N را تولید می‌کند، بطوریکه $x < N$ و $2 \le r < N$. مقدار r را کلید خصوصی در نظر می گیرد و مقدار $T_r(x)$ را حساب می‌کند و مقادیر x، N و $T_r(x)$ را به گره مقابل مثلا گره B می‌فرستد.

گره B یک مقدار تصادفی (کلید خصوصی) مانند s $(2 \le s < N)$ را به صورت امن تولید می‌کند و مقدار $T_s(x)$ را محاسبه می‌کند و مقدار آن را به گره A می‌فرستد سپس مقدار کلید مشترک را با استفاده از ترکیب توابع مانند زیر حساب می‌کند.

$$K = T_s(T_r(x)) \mod N$$

و گره A نیز به روش مشابه مقدار کلید مشترک را مانند زیر حساب می‌کند(که با توجه به رابطه (۳) برابر با K خواهد شد).

$$K' = T_r(T_s(x)) \mod N$$

[1] Semi-group

۲–۸ مساله لگاریتم گسسته بر اساس نگاشت آشوب چبیشف

با فرض عناصر x و y مساله لگاریتم گسسته بر اساس نگاشت آشوب چبیشف بیان می‌کند که پیدا کردن مقداری r از رابطه $T_r(x)\equiv y$ امکان پذیر نیست.

۲–۹ مساله دیفی–هلمن بر اساس نگاشت آشوب چبیشف

مساله دیفی-هلمن بر اساس چندجمله‌ای چبیشف (چند جمله‌ای بهبودیافته) بیان می‌کند که با در دست داشتن چندجمله‌ای‌های $T_r(x)$ و $T_s(x)$ ، پیدا کردن ترکیب $T_{rs}(x)$ بدون داشتن مقادیر r و s امکان پذیر نیست.

۲–۱۰ تابع درهم ساز یک طرفه[1]

تابع درهم، یک تابع یک‌طرفه است که ورودی با طول متغییر را گرفته و خروجی با طول ثابتی را تولید می‌کند یک تابع درهم یک‌طرفه باید چهار خصوصیت زیر را داشته باشد[۲۰,۱۸].

(۱). تابع درهم h(.) برای همه کاربران مشخص شده است حتی برای حمله کننده

(۲). بصورت موثر بتوان برای پیام دلخواه M مقدار h(m) را محاسبه کرد.

(۳). چنانچه کاربر غیر مجاز مقدار h(m) را در اختیار داشته باشد امکان محاسبه مقدار m از روی آن در زمان منطقی امکان‌پذیر نباشد.

(۴). تابع درهم ساز باید عدم تصادم بصورت ضعیف را فراهم کند. تابع را بصورت ضعیف بدون تصادم[2] گویند اگر پیدا کردن یک تصادم برای پیام x از نظر محاسباتی سخت باشد. به عبارت دیگر پیدا کردن یک پیام y که $x\neq y$ به نحوی که $h(x) = h(y)$ از نظر محاسباتی در زمان منطقی غیر ممکن باشد.

۲–۱۱ خاصیت Unlinkability

خاصیت Unlinkability دو یا چند آیتم به این معنی است که در یک سیستم حمله کننده نمی‌تواند به صورت موثر تشخیص دهد که آیا این آیتم‌ها به هم مرتبط هستند یا نه.

[1] One-way hash function
[2] Weakly collision free