طراحی مدل سایبرنتیک الگوریتم‌های رمزنگاری و رتبه‌بندی مؤلفه‌های پشتیبان آن با استفاده از روش ELECTRE III

علی‌محمد نوروززاده گیل ملک [۱]، محمدرضا عارف [۲*]، رضا رمضانی خورشیددوست [۳]
دانشکده مهندسی برق دانشگاه صنعتی شریف،
دانشکده مهندسی صنایع دانشگاه صنعتی امیرکبیر،

چکیده:

تحقق امنیت مطلوب و پایدار در شبکه‌های برخوردار از گستره ملی، سازمانی و حتی در سامانه‌های اطلاعاتی دارای حساسیت، باید مبتنی بر یک روش نظام‌مند و همه جانبه‌نگر بوده و به‌صورت گام‌به‌گام انجام گیرد. رمزنگاری مهم‌ترین سازوکار برای تأمین امنیت اطلاعات بوده که بیش‌تر مبتنی بر الگوریتم‌های رمزنگاری است. در طراحی یک الگوریتم همه مؤلفه‌های لازم امنیت را باید در یک الگوی متعالی از جنبه‌های فنی، سازمانی، رویه‌ای و انسانی در نظر گرفت. برای پاسخ‌گویی به این نیازها، ابتدا باید برپایهٔ یک مدل، مؤلفه‌های مؤثر را استخراج و سپس میزان تأثیر مؤلفه‌ها را تعیین کرد. در این مقاله از روش‌شناسی سایبرنتیک برای تهیه یک اَبَرمدل استفاده می‌کنیم. فعل و انفعالات مؤلفه‌های این ابر مدل یک گراف پیچیده تشکیل می‌دهند. جهت غلبه بر این پیچیدگی، برای تعیین اولویت مؤلفه‌های آن از ابزار ELECTRE III استفاده می‌کنیم. نتایج حاصل از آن با درصد بالایی منطبق بر گزارش‌های منتشرشده توسط ITU در سال‌های ۲۰۱۵، ۲۰۱۷ و ۲۰۱۸ است.

واژگان کلیدی: الگوریتم‌های رمزنگاری، ابرمدل، سایبرنتیک، MCDM، ELECTRE III.

Design of cybernetic metamodel of cryptographic algorithms and ranking of its supporting components using ELECTRE III method

Ali Mohammad Norouzzadeh Gil Molk[1], Mohammad Reza Aref[2]*, Reza Ramazani Khorshiddoust[3]

Department of Computer Engineering, Islamic Azad University, North Tehran Branch
Department of Electrical Engineering, Sharif University of Technology
Amirkabir University of Technology

Abstract

Nowadays, achieving desirable and stable security in networks with national and organizational scope and even in sensitive information systems, should be based on a systematic and comprehensive method and should be done step by step. Cryptography is the most important mechanism for securing information. a cryptographic system consists of three main components: cryptographic algorithms, cryptographic keys, and security protocols, which are mainly based on cryptographic algorithms. In designing a cryptographic algorithm, all the necessary components of information security must be considered in a model of excellence in technical, organizational, procedural and human aspects. To meet these needs, we must first extract the effective components in the design and implementation of cryptographic algorithms based on a model and then determine the impact of the components. In this paper, we use cybernetic methodology to prepare a metamodel .The cryptographic cybernetics

* نویسندهٔ عهده‌دار مکاتبات
* Corresponding author

• تاریخ ارسال مقاله: ۱۳۹۹/۶/۱۴ • تاریخ پذیرش: ۱۳۹۹/۷/۳۰ • تاریخ انتشار: ۱۴۰۱/۱۲/۲۹ • نوع مطالعه: پژوهشی

metamodel has four components: “strategy / policy ", "main process", "support process" and "control process". The "main process" has four stages and also, the "suport process" includes 13 components of hardware and software. The interactions of these two processes shape its structure, leading to a complex graph. To prioritize suport components for resource allocation and cryptography strategy, it is necessary to rank these components in the designed metamodel. To overcome this complexity in order to rank the support components, we use the ELECTRE III method, which is a multi-criteria decision-making method. The results show that the components with high priority for the development of the cryptographic system are: Research and Development, Human Resources, Management, Organizational, Information and Communication Technology, Rrules and Regulations and standards. These results are consistent with reports published by the ITU in 2015, 2017 and 2018 .

Keywords: Cryptographic algorithms, Metamodel, Cybernetics, MCDM, ELECTRE III

۱- مقدمه

فناوری اطلاعات و ارتباطات به‌عنوان یک فناوری عمده و توانمندساز برای دستیابی به اهداف کلان توسعه پایدار در هر کشوری، نقش محوری ایفا می‌کند. به گفته Kenneth Geers، نویسنده استراتژیک امنیت سایبری [1]، وجه غالب امنیت ملی در سال ۲۰۲۵ وابسته به توسعه فناوری اطلاعات بوده و رمزنگاری مهم‌ترین سازوکار برای ارتقای سطح امنیت اطلاعات است. در [2] گرایش عمومی به رمزنگاری در بخش‌های مختلف صنعت مورد بررسی قرار گرفته است که نشان‌می‌دهد در سال ۲۰۰۵، ۱۵ درصد سازمان‌ها و در سال ۲۰۱۷، ۴۳ درصد دارای یک استراتژی رمزنگاری هستند. هر سامانهٔ رمزنگاری شامل سه بخش الگوریتم‌های رمزنگاری، کلیدهای رمزنگاری و پروتکل‌های امنیتی است که الگوریتم‌های رمزنگاری اساس این سامانهبوده [3] و قدرت آن وابستگی شدیدی به طراحی و پیاده‌سازی الگوریتم‌ها، خواص نظری، صحت و قدرت اجرای آنها در سخت‌افزار و نرم‌افزار دارد [4].

در ۲۰۱۶، NIST[1] استانداردها و دستورالعمل‌های توسعه الگوریتم‌های رمزنگاری را تدوین کرد که مواردی همچون شفافیت[۲]، بازبودن[۳]، متعادل‌بودن[۴]، صحت[۵]، ارزش فنی[۶]، مقبولیت جهانی[۷]، قابل‌استفاده‌بودن[۸]، توسعه مداوم[۹]و نوآوری و مالکیت معنوی[۱۰] از اصول آن هستند [5]. همچنین مجموعه‌ای از الگوریتم‌های رمزنگاری سبک‌وزن را برای استفاده در دستگاه‌های محدودشده طراحی کرد [6]. در [7] شاخص‌های امنیت، هزینه، کارایی و ویژگی‌های پیاده‌سازی به‌عنوان معیار اصلی ارزیابی در نظر گرفته شده‌است. در [8] سیاست‌ها و فرآیندهای مدیریت چرخه حیات استانداردهای الگوریتم رمزنگاری ارائه و در [9] یک چارچوب تحلیلی برای پیاده‌سازی سخت‌افزار و نرم‌افزار با برنامه‌های رمزنگاری، ارائه شده‌است. CSRC[11] در سال ۲۰۱۸ مطلبی تحت عنوان برنامه اعتبارسنجی الگوریتم رمزنگاری یا CAVP[12] را منتشر کرد [10].

هر چند در نگاه نخست، الگوریتم‌های رمزنگاری برای دسترسی به اهدافی همچون، محرمانگی، اصالت و جامعیت طراحی می‌شوند [11] اما باید مؤلفه‌های زیادی همچون سرعت، مصرف منابع، نوع کاربری و غیره را در نظر گرفت. تأمین همه آنها به‌طور همزمان، امری مشکل و گاه غیرممکن است. در حالت ایده‌آل، کاربر نیاز به الگوریتمی دارد که هزینه کم و کارایی بالا داشته‌باشد [12] اگر در طراحی، اهداف متناقضی در نظر گرفته شوند، بیش‌تر الگوریتم‌ها شکسته می‌شوند [13]. در طراحی الگوریتم‌ها، از فناوری‌های مختلفی از جمله مهندسی اجتماعی، علوم ریاضی، سیگنال‌های فیزیولوژیکی و بیومتریک استفاده می‌شود [15] ,[14].

اغلب کشورها سعی دارند برای تأمین امنیت سرویس‌های زیرساختی و اطلاعات طبقه‌بندی شده از الگوریتم‌های بومی استفاده کنند. در این مقاله ضمن شناسایی عوامل مؤثر در طراحی الگوریتم‌های رمزنگاری، برای تخصیص منابع به‌صورت هدفمند در راستای ارتقای دانش این حوزه، این عوامل رتبه‌بندی شده‌اند. برای تحقق امنیت مطلوب، لازم است همه مؤلفه‌های امنیت در ابعاد فناورانه، سازمانی، فرایندی و انسانی [16]، به‌صورت متناسب ایجاد شده و برپایهٔ یک مدل تعالی توسعه یابند تا سطح قابل قبولی از امنیت، استقرار و استمرار یابد [18][17]. برای دست‌یابی به این هدف باید مدلی جامع و کاربردی ارائه کرد.

[1] National Institute of Standards and Technology
[2] Transparency
[3] Openness
[4] Balance
[5] Integrity
[6] Technical Merit
[7] Global Acceptability
[8] Usability
[9] Continuous Improvement
[10] Innovation and Intellectual Property (IIP)
[11] Computer Security Resource Center
[12] Cryptographic Algorithm Validation Program

۲- روش شناسی پژوهش

با توجه به وجود معیارهای مختلف فنی و غیر فنی در فرایند طراحی الگوریتم‌های رمزنگاری، جهت تعیین دقیق معیارها (مؤلفه‌ها)، ابتدا با استفاده از روش‌شناسی سایبرنتیک[1] مدل مفهومی طراحی الگوریتم‌های رمزنگاری را به‌دست آورده و سپس برای رتبه‌بندی مؤلفه‌های مورد نیاز از روش ELECTRE[2] III که یکی از مجموعه روش‌های تصمیم گیری چندمعیاره[3] (MCDM)) است استفاده می‌نماییم، زیرا این روش هم از مدل‌های ریاضی و هم از نظرات تصمیم گیرندگان[4] برای تحلیل استفاده می‌کند.

۲-۱- روش‌شناسی سایبرنتیک

رویکرد سیستمی با استفاده از مفهوم سلسله‌مراتبی سبب می‌شود تا از پرداختن بی‌مورد به جزئیات مزاحم خودداری شده و به روابط بین مؤلفه‌ها توجه ویژه شود. هر چه پیچیدگی مدل بیشتر باشد، پیاده‌سازی "مؤلفه‌ای" مفیدتر خواهد بود. به‌عبارت دیگر، اجزای مدل را باید به‌صورت "مؤلفه‌ای" طراحی و ساخت. البته باید دقت کرد که اثرهای متقابل اجزا نیز در نظر گرفته شوند. مدل راهبردی برای طراحی الگوریتم‌های رمزنگاری باید در سطحی از جزئیات ارائه شود که میان معیارهای "شمول" و کاربردپذیری مصالحه کند. منظور از "شمول"، دربرگیرندگی الگوریتم‌های مختلف رمزنگاری است. منظور از "کاربردپذیری"، قابلیت بالقوه به‌کارگیری آن در سطح ملی برای افزایش سطح امنیت فناوری ارتباطات و اطلاعات است؛ علاوه‌براین، مدلی که ارائه می‌شود، می‌بایست از "استواری منطقی" برخوردار باشد. منظور از "استواری منطقی"، سازگاری[5] عوامل و روابط داخلی مدل است. برای پاسخ‌گویی به این نیازها، در این مقاله ما از روش‌شناسی سایبرنتیک برای تهیه یک ابر مدل[6] استفاده می‌کنیم که سلسله‌مراتبی، شفاف، کنترل‌پذیر و قادر به هم‌گرایی اهداف است. این ابر مدل سایبرنتیک دارای چهار مؤلفه توسعه راهکار / راهبرد[7]، فرایند اصلی[8]، فرایند پشتیبانی[9] و کنترل‌های فرایند / فراورده[10] است.

در [19] سایبرنتیک را به‌معنای ارتباط و کنترل در سامانه‌های پیچیده از طریق تمرکز بر سازوکارهای بازخورد یا چرخه‌ای معرفی می‌کند. بر این پایه مهم‌ترین اصول الگوی سایبرنتیک عبارتند از: پیچیدگی[11]، متقابل‌بودن[12]، تکامل‌پذیری[13]، ساختارمندی[14] و بازگشت‌پذیری[15]؛ بنابراین، مدل عمومی سایبرنتیک مبتنی بر کنترل کلاسیک است و می‌توان آن را برای سامانه‌های پیچیده‌ای همچون طراحی و پیاده‌سازی الگوریتم‌های رمزنگاری که عوامل متعدد و گاه متضاد در آن نقش دارند، استفاده‌کرد. این مدل به‌اندازه کافی روش‌مند و نظام‌مند است؛ زیرا به‌لحاظ فیزیکی قابل‌درک، جامع، سلسله‌مراتبی و دارای ساختار گراف، نمودار و ابزار تجزیه و تحلیل همگرایی است. [26–20].

۲-۱-۱- مدل کلی طراحی الگوریتم‌های رمزنگاری برپایهٔ روش‌شناسی سایبرنتیک

مدل کلی سایبرنتیک برای طراحی الگوریتم‌های رمزنگاری برپایهٔ چهار مؤلفه طراحی شده‌است:

فرایند اصلی: این نوع فرآیند شامل علت ایجاد و یا وجودی سامانه است. این فرایند سه نوع الگوریتم رمزنگاری متقارن، نامتقارن و توابع چکیده‌ساز را شامل می‌شود.

فرایند توسعه راه‌کار / راهبرد: در این فرایند، با توجه به راه‌کارها و راهبردهای مورد انتظار و تأییدشده در سامانه، می‌توان مبنای کارکردی و مقایسه‌ای (مانند مقادیر مرجع یا استاندارد) را تعیین و طراحی کرد.

فرآیند پشتیبانی: این فرایند نزدیک‌ترین مجموعه‌فرایندها به فرایند اصلی است و برای تحقق فرایند اصلی "لازم" است. فرایند پشتیبانی به دو دستهٔ سخت‌افزاری و نرم‌افزاری تقسیم می‌شود. فرایند پشتیبانی سخت‌افزاری، مجسم[16] و به‌لحاظ کمّی سنجش‌پذیر[17] است، که عبارتند از: توسعه و تأمین تجهیزات[18]، مواد[19] و زیرساخت[20]. فرآیند پشتیبانی نرم‌افزاری، مجسم نیست،

[1] Cybernetic
[2] Elimination Et Choice Translating REality
[3] Multiple Criteria Decision Making
[4] Decision Maker
[5] consistency
[6] Meta Model
[7] strategy/policy development
[8] Main Process or Core Process
[9] Supportive Process
[10] Process / Product
[11] Complexity
[12] Mutuality
[13] Evolvability
[14] constructivity
[15] Reversibility
[16] concrete
[17] measurable
[18] Equipment
[19] Material
[20] Infrastructure

ولی اغلب سنجش‌پذیر است که عبارتند از: مدیریت[1]، سازمان / ساختار[2]، منابع انسانی / آموزش[3]، تحقیق و توسعه[4] (R&D)، استانداردسازی، قانون و مقررات[5]، منابع مالی[6]، فناوری‌های ارتباطات و اطلاعات یا فاوا[7] (ICT)، روابط‌عمومی و بین‌المللی[8] و فرهنگ[9].

کنترل فرایند و فراورده (فرآیند بازخورد)[10]: این فرایند شامل کنترل فرایند طراحی و پیاده‌سازی الگوریتم‌های رمزنگاری و همچنین فرایند مربوط به کنترل محصول تولید شده‌است.

این مدل به هر دو جنبه‌ی "ساختاری" و "فرایندی" الگوریتم‌های رمزنگاری می‌پردازد. منظور از "ساختار"، چینش سطح‌مند عوامل مؤثر بر رمزنگاری است. همچنین منظور از فرایند، مجموعه‌ای سطح‌مند از فعالیت‌ها است که با منطقی مشخص، مجموعه‌ای از ورودی‌ها را به مجموعه‌ای از خروجی‌ها تبدیل می‌کنند. منطق به‌صورت مجموعه‌ای همخوان مفاهیم و قواعد تعریف می‌شود که منظور از همخوان، عدم وجود ناسازگاری است. با توجه به مؤلفه‌های استخراج شده برای هر یک از بخش‌های اصلی، نرم‌افزاری، سخت‌افزاری و کنترلی، می‌توان مدل سایبرنتیک طراحی و پیاده‌سازی الگوریتم‌های رمزنگاری را به شکل (۱) رسم کرد.

فرایند اصلی این مدل شامل گام‌های طراحی الگوریتم‌های رمزنگاری است که سیاست‌ها و فرآیندهای مدیریت چرخه حیات آن به‌صورت زیر پیشنهاد می‌شود [5].

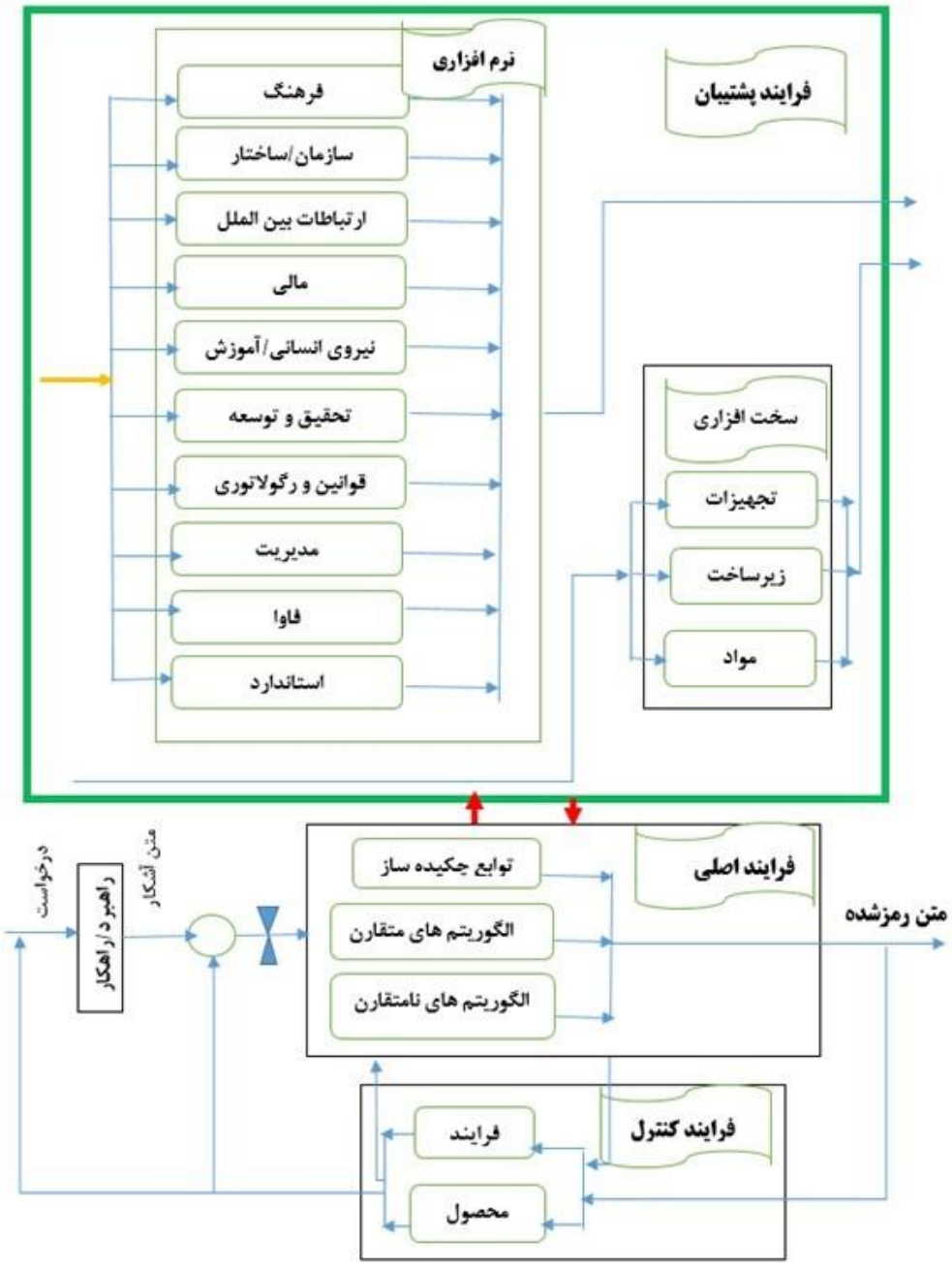
۱- شناسایی و ارزیابی نیاز که خود شامل این موارد است: تعیین نوع کاربری، آیا یک دستورالعمل قانونی یا اداری وجود دارد؟ آیا پیشرفت فناوری معین، منافع خاصی را به‌دنبال دارد؟
۲- اعلام استفاده از یک استاندارد یا دستورالعمل پروژه که خود می‌تواند شامل برگزاری مسابقه یا اعلام عمومی و فراخوان از متخصصان باشد.
۳- توجه به نیازمندی‌ها و راه‌حل‌ها که خود می‌تواند شامل مواردی همچون تعیین ویژگی‌های امنیتی مطلوب و معیارهای ارزیابی برای ارزیابی راه‌حل‌های بالقوه، تحقیق درباره‌ی ادبیات و آنچه که درقبل در محصولات و استانداردها آمده است، ارائه اثبات‌های امنیتی برای الگوریتم‌ها یا طرح‌های پیشنهادی باشد.
٤- تعیین یک برنامه و فرآیند مشخص که خود شامل بررسی الگوریتم‌های موجود با توجه به نیازمندی‌ها جهت بهبود (درصورتی‌که با بهبود به هدف برسیم)، طراحی یک الگوریتم جدید با توجه به نیازمندی‌ها (درصورتی‌که بهبود یک الگوریتم موجود، باعث دستیابی به هدف نمی‌شود) است.
٥- طراحی و توسعه استاندارد با همکاری متخصصان دانشگاهی، صنعت و دولت.
٦- ارزیابی استاندارد که شامل آزمون‌های امنیتی و شناسایی روش‌های نفوذ و شکستن رمز است.
۷- نگهداری استاندارد که خود شامل بازبینی، به‌روزرسانی و یا صرفنظر کردن از آن است.

برپایهٔ فرایندها و نیازمندی‌های هفت‌گانه اصلی بیان شده و همچنین دسته‌بندی آنها، گام‌های طراحی و پیاده‌سازی الگوریتم‌های رمزنگاری فارغ از دسته‌بندی سه‌گانه توابع چکیده‌ساز، متقارن و نامتقارن، در بالاترین سطح، در شکل (۲) نشان داده شده‌است.

۲-۲- تصمیم‌گیری چندمعیاره یا MCDM

فنون تصمیم‌گیری، مجموعه روش‌هایی است که جهت ارزیابی راه‌حل‌های موجود و انتخاب بهترین راه‌حل به کار می‌رود. تصمیم‌گیری چندمعیاره یک چارچوب برای ارزیابی مسائل چندبُعدی، متناقض و ناسازگار بوده و بیان‌گر شرایطی است که معیارهای چندگانه (کمی و کیفی) اما غالباً متعارض در تصمیم‌گیری وجود دارند [27]. این مدل در حوزه‌های مختلف مورد استفاده قرار گرفته است [35–28]. روش‌های بهینه‌سازی چندمعیاره، علمی جدید بوده که برای اولین بار در کارهای کوپمن [36]به اصطلاحِ مؤثر[11] اشاره‌شده است. کان و تشکر [37] مسئله بزرگ‌ترین بردار را در این حوزه معرفی کرده و جنبه‌های الگوریتمی آن برای اولین بار توسط چارنز و کوپر [38] مطرح شد. در سال ۱۹۶۸ مفهوم رتبه‌بندی و روش تصمیم‌گیری چندمعیاره گسسته الکتره[12] [39] به‌طور جامع مطرح شد. اولین روش‌های تعاملی یعنی روش است[13] [40] و روش جیوفریون - دایر – فینبرگ [41] در دهه ۷۰ مطرح شدند.

[1] management
[2] Organization / Structure
[3] Human resource / Education
[4] Research and Development
[5] rule and regulation
[6] financial resource
[7] Information and Communication Technology (ICT)
[8] public/international relations
[9] cultural
[10] Process/Product Control (Feedback Process)
[11] efficient
[12] ELECTRE
[13] STEM



(شکل- ۱): مدل سایبرنتیک طراحی و پیاده‌سازی الگوریتم‌های رمزنگاری

(Figure-1): Cybernetic model design and implementation of cryptographic algorithms

(شکل-۲): گام‌های فرایند اصلی طراحی و پیاده‌سازی الگوریتم‌های رمزنگاری در بالاترین سطح

(Figure-2): The main process steps of designing and implementing cryptographic algorithms at the highest level

۲-۲-۱- روش ELECTRE III

رویه‌هایی برای انتخاب روش مناسب تصمیم‌گیری چندمعیاره توسط افرادی نظیر هوبز، اوزرنوی، هوا نگو یون ارائه شده‌است [45–42]. این رویه‌ها عمدتاً برپایهٔ اطلاعات ورودی و تعداد معیارهای مورد نیاز ارائه شده‌اند. در این مقاله از روش ELECTRE III استفاده می‌شود. این روش در حوزه‌های مختلفی همچون مدیریت و بهینه‌سازی سیستم‌های انرژی [46]، رتبه‌بندی بهینه گزینه‌های منابع آب [47]، انتخاب سامانه مدیریت پسماندها [48]، رتبه‌بندی پروژه‌ها از لحاظ سودآوری [49]، برنامه‌ریزی منابع طبیعی استراتژیک [50] استفاده‌شده است. روش Electre III، مانند هر روش برون‌گرا، مبتنی بر بدیهی‌بودن مقایسه جزئی است که براساس آن، ترجیحات با استفاده از سه معیار آستانه ارجحیت[1](P) ، آستانه بی‌تفاوتی[2] (q) و آستانه رد[3] (v) مورد بررسی قرار می‌گیرند.

۲-۲-۲- گام‌های ELECTRE III:

برای درک بهتر این روش، مراحل اجرای آن به‌صورت گام به گام آورده می‌شود:

گام **۱- تشکیل ماتریس تصمیم:** برپایهٔ داده‌های به‌دست‌آمده و تعامل بین مؤلفه‌های پشتیبان و گام‌های فرایند اصلی، ماتریس تصمیم به‌شکل کلی رابطه (۱) تشکیل‌می‌شود:

$$\mathbf{X} = \begin{vmatrix} r_{11} & \dots & r_{1n} \\ \dots & \dots & \dots \\ r_{m1} & \dots & r_{mn} \end{vmatrix} \qquad (۱)$$

که در آن درایه x_{ij} عملکرد گزینهi ام در رابطه با معیارj ام می‌باشد.

گام **۲- بی‌مقیاس[4]کردن ماتریس تصمیم:** برای قابل‌مقایسه‌شدن مقیاس‌های مختلف اندازه‌گیری به‌ازای معیارهای گوناگون، ماتریس تصمیم باید بی‌مقیاس شود تا عناصر شاخص‌های تبدیل‌شده (X_{ij}) بدون بُعد اندازه‌گیری شوند. برای این‌منظور، روش‌های مختلفی مانند نُرم، خطی و فازی وجود دارد که در این مقاله از روش نُرم (رابطه ۲) استفاده‌شده است.

$$r_{ij} = \frac{X_{ij}}{\sqrt{\sum_{i=1}^{m} {X_{ij}}^2}} \qquad (۲)$$

گام **۳- تعیین وزن معیارها:** با توجه به ضرایب اهمیت معیارهای مختلف در تصمیم‌گیری، بردار ضریب اهمیت (W) تعیین می‌شود که مجموع آن برابر یک است. وزن معیارها را می‌توان از روش‌های مختلفی مانند آنتروپی شانون، LINMAP[5]، کمترین مجذورات و بردار ویژه محاسبه کرد که در این مقاله از روش آنتروپی شانون استفاده‌شده است.

گام **۴- تشکیل ماتریس تصمیم وزن‌دار هنجار[6]شده:** ماتریس تصمیم وزن‌دار، از ضرب ماتریس تصمیم بی‌مقیاس‌شده در بردار وزن معیارها (W) به‌دست می‌آید (رابطه ۳).

$$V_{ij}=w_j \times r_{ij} \quad j=1, 2\dots n;\ i=1, 2\dots m \qquad (۳)$$

V_{ij} : ماتریس تصمیم وزن‌دار

W_j: بردار وزن حاصل از ماتریس تصمیم بی‌مقیاس شده

گام **۵: تعریف مقادیر آستانه:** به‌منظور ایجاد یک رابطه ارجحیت در ELECTRE III ، ابتدا سه مقدار آستانه، یعنی آستانه بی‌تفاوتی(q_j) ، آستانه ارجحیت (p_j) و آستانه رد(v_j) معرفی می‌شوند به‌طوری‌که برای معیار تصادفی C_i داریم: $0<q_i<p_i<v_i$. مقادیر سه آستانه اغلب توسط تصمیم‌گیرندگان مشخص می‌شود، اما در این مقاله جهت جلوگیری از اعمال سلیقه و کاهش ضریب خطا، برپایهٔ [51] و رابطه موجود بین آنها به‌دست می‌آید.

آستانه بی‌تفاوتی (q_j): اگر ارزش دو گزینه در یک معیار مشخص تفاوت ناچیزی داشته‌باشند هر دو گزینه انتخاب می‌شوند ولی اگر ارزش گزینه‌ها به محدوده بی‌تفاوتی برسد یکی از آن‌ها انتخاب می‌شود؛ بنابراین محدوده بی‌تفاوتی نشان‌دهندهٔ عدم برتری یک گزینه نسبت به گزینهٔ دیگر است، یعنی در آن محدوده دو گزینه در برآوردن معیاری معلوم هیچ برتری نسبت به‌هم ندارند. رابطه $r_{ij} <= r_{kj} + q_j$ و $r_{kj} <= r_{ij} + q_j$ در معیار c_j بین آنها برقرار است و مقدار آن از رابطه (۴) به‌دست می‌آید.

(۴)

$$q_j = (\text{حداقل مقدار مؤلفه} - \text{حداکثر مقدار مؤلفه}) * \%m$$

دامنه %m به‌طورمعمول از ۵ تا ۱۰ متغیر است که در این مقاله مقدار آن ۱۰٪ در نظر گرفته شده‌است.

آستانه ارجحیت (P_j): اگر ارزش گزینه‌ای در معیار C_j به اندازه‌ی آستانه ارجحیت باشد، آن گزینه برتر خواهد

[1] Preference Threshold
[2] Indifference Threshold
[3] Veto Threshold
[4] Dimensionless

[5] Linear-Programming for multidimensional analysis of preference
[6] normal

بود. به‌عبارتی اگر $r_{ij}-r_{kj}> =p_j$، گزینه a_i نسبت به a_k ارجحیت دارد. مقدار این آستانه از رابطه ۵ به‌دست می‌آید:

$$p_j = (q_j*K) \quad (۵)$$

مقدار K اغلب بین ۳ تا ۱۰ متغیر است که در این مقاله مقدار ۳ در نظر گرفته شده‌است.

آستانه رد (v_j): وقتی اختلاف دو گزینه در معیار مشخص C_j کمتر از v_j نیست، یعنی $r_{ki}> =r_{ij}+v_i$ در این‌صورت گزینه (مؤلفه) a_i نسبت به a_k برتری ندارد. مقدار آن از رابطه ۶ به‌دست می‌آید.

$$v_j = (\text{حداقل مقدار مؤلفه} - \text{حداکثر مقدار مؤلفه})*L \quad (۶)$$

دامنه L بین ۳ تا ۵ است که در این مقاله مقدار ۳ در نظر گرفته شده‌است.

گام ۶: محاسبه ماتریس هماهنگی[1]: با استفاده از رابطه ۷، مقادیر ماتریس هماهنگی C (a,b) را محاسبه می‌نماییم که نشان‌دهنده میزان برتری گزینه a نسبت به گزینه b است..

$$C(a,b) = \frac{\sum_{i=1}^{m} W_i C_i(\text{a,b})}{\sum_{i=1}^{m} W_i} \quad (۷)$$

در این رابطه c_i *(a,b)* مجموعه هماهنگ یا تطابق[2] گزینه‌های a و b در معیار i است میزان سطح برتری را در آن معیار مشخص می‌کند. مقدار آن برپایهٔ رابطه ۸ به‌دست می‌آید.

$$C_i(a,b) = \begin{cases} 0 & if\ g_i(b) - g_i(a) \geq p_i(g_i(a)) \\ 1 & if\ g_i(b) - g_i(a) \leq q_i(g_i(a)) \\ \frac{p_i + g_i(\text{a}) - g_i(\text{b})}{p_i - q_i} & Otherwise \end{cases} \quad (۸)$$

که در آن g_i*ها* درایه‌های ماتریس هستند.

گام ۷: محاسبه ماتریس ناهماهنگ[3]: با استفاده از رابطه ۹، مقادیر ماتریس مغلوب d (a,b) را محاسبه می‌نماییم. این ماتریس نشان می‌دهد که عدم برتری یک گزینه نسبت به دیگری در قبال معیارهای دیگر به چه میزان است؛ بنابراین در قبال یک معیار خاص، هر چه شاخص توافق بیشتر و عدم‌توافق کمتر باشد، به‌منزله برتری قوی‌تر خواهد بود.

$$D(a,b) = \frac{\sum_{i=1}^{m} W_i d_i(\text{a,b})}{\sum_{i=1}^{m} W_i} \quad (۹)$$

در این رابطه d_i *(a,b)* شاخص‌های ناهماهنگ یا عدم تطابق[4] گزینه‌های a و b در معیار i است که برپایهٔ رابطه ۱۰ به‌دست می‌آید.

$$d_j(a,b) = \begin{cases} 0 & if\ \ g_i(a) + p_j \geq g_j(b) \\ 1 & if\ \ g_j(a) + v_j \leq g_j(b) \\ \frac{g_j(b) - g_j(a) - p_j}{v_j - p_j} & Otherwise \end{cases} \quad (۱۰)$$

گام ۸: محاسبه ماتریس اعتبار[5]: برای هر جفت از مؤلفه‌های طراحی الگوریتم $(a,\ b) \in A$، مقادیر هماهنگ و ناهماهنگ وجود دارد. مرحله آخر ساخت مدل، ترکیب این دو مقدار برای تعیین رتبه‌بندی بین مؤلفه‌ها است. یعنی، ماتریس اعتبار قدرت این ادعا را ارزیابی می‌کند که "a حداقل به‌اندازه b خوب است". ماتریس اعتبار برای هر جفت (a, b) برپایهٔ رابطه ۱۱ محاسبه می‌شود.

$$S(a,b) = \begin{cases} C(a,b),\ if\ d_j(a,b) \leq C(a,b) \forall j \\ C(a,b).\prod_{j \in J(a,b)} x = \frac{1 - d_j(a,b)}{1 - C(a,b)} \end{cases} \quad (۱۱)$$

که در آن $J\ (a,b)$ مجموعه معیارهایی هستند که در آن $d_j(a,\ b) > C(a,\ b)$ است.

گام ۹: رتبه‌بندی مؤلفه‌ها: برای این منظور پارامتر λ را به‌صورت رابطه ۱۲ تعریف می‌کنیم:

$$\lambda = \text{Max S (a,b)} ;\ \text{a, b} \in \text{A} \quad (۱۲)$$

این پارامتر مقدار اعتباری را معین می‌کند که تنها مقادیری از S (a,b) که نزدیک به λ هستند مورد توجه قرار گیرند. در این فرایند پارامتر جدیدی به نام s (λ) معرفی می‌شود که از رابطه ۱۳ به‌دست می‌آید. مقادیر α و β در آنالیز حساسیت تغییر کرده و مقدار پیش فرض آنها ۰/۰۱ و ۰/۰۳ است.

$$S(\lambda) = \alpha\lambda + \beta \quad (۱۳)$$

با محاسبه λ-S (λ) ماتریس T به‌صورت رابطه ۱۴ به‌دست می‌آید.

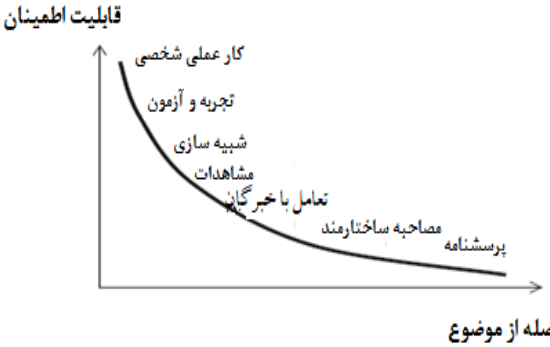
$$T(a,b) = \begin{cases} 1, & if\ S(a,b) > \lambda - S(\lambda) \\ 0, & Otherwise \end{cases} \quad (۱۴)$$

در نهایت مطلوبیت برای هر گزینه با Q (a) نشان داده‌می‌شود که به معنی تعداد گزینه‌هایی است که گزینه a نسبت به آنها برتر بوده من‌های گزینه‌هایی که نسبت به a برتر بوده‌اند. به‌عبارتی؛ Q (a) به‌صورت مجموع اعداد سطرها من‌های مجموع اعداد ستون‌های ماتریس T برای هر گزینه تعریف می‌شود. گزینه‌های دارای اعداد بزرگ‌تر، اولویت بیشتری دارند.

[1] Concordance Matrix
[2] Concordance
[3] Discordance Matrix
[4] Discordance index
[5] Credibility Matrix

۳ - جمع آوری داده‌ها

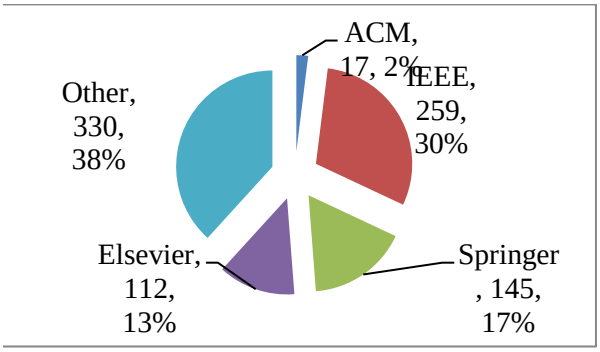
برای طراحی یک الگوریتم رمزنگاری سلسله‌مراتبی کارآمد، عوامل مهم باید به‌درستی شناسایی، انتخاب و گروه‌بندی شوند. برای دست‌یابی به مجموعه داده معتبر، روش‌های مختلفی وجود دارد که برپایهٔ [52] قابلیت اطمینان آنها در شکل (۳) نشان داده شده‌است. در این مقاله از روش مشاهده[1] برای بازه زمانی ۲۰۱۹-۱۹۸۷ و [53] استفاده‌شده است.



(شکل-۳): میزان قابلیت اطمینان هر یک از روش‌های جمع‌آوری اطلاعات [52]

(Figure-3): Reliability, depending on the investigation method used [52]

بعد از بررسی محتوای داده‌های به‌دست آمده، تعداد ۸۶۳ مقاله، مستند و گزارش فنی که مربوط به طراحی و پیاده‌سازی الگوریتم‌های رمزنگاری انتخاب شدند. میزان فراوانی آنها بر حسب انتشار در مراجع معتبر در شکل (۴) آورده شده‌است که ۶۲ درصد منابع استفاده‌شده، از چهار مرجع معتبر علمی IEEE (۳۰٪)، Springer (۱۷٪)، Elsevier (۱۳٪) و ACM (۲٪) می‌باشند. بقیه این مستندات نیز از مراجعی همچون NIST، ITU و نیز مسابقات برگزار شده بین المللی مانند ECRYPT استخراج شدند.



(شکل-۴): درصد انتشار مقالات، مستندات و گزارشات فنی در مراجع مختلف

(Figure-4): Percentage of publishing papers, documents and technical reports in various sources

برپایهٔ مدل سایبرنتیک، ۱۳ مؤلفه برای فرایند پشتیبان تعریف شدند. برای دست‌یابی به ارتباط بین مؤلفه‌های پشتیبان و گام‌های طراحی الگوریتم، ماتریسی با اندازه ۱۳×۴ تشکیل می‌دهیم که سطرهای آن مؤلفه‌های فرایند پشتیبان و ستون‌های آن عناصر چهارگانه فرایند اصلی است. برپایهٔ داده‌های جمع‌آوری‌شده، هر درایه این ماتریس برپایهٔ منابع اشاره‌شده، در محدوده صفر تا ۱۰ مقداردهی می‌شود جدول (۱). اعداد هر درایه میزان تأثیر هر مؤلفه پشتیبان بر هر مرحله از طراحی را نشان‌می‌دهد. به‌عنوان مثال عدد هشت در درایه منابع انسانی-کاربری نشان دهنده تأثیر ۸۰ درصدی مؤلفه پشتیبان منابع انسانی در تعیین نوع کاربری یک الگوریتم رمزنگاری است. تحلیل این ماتریس و محاسبات مدل‌سازی آن، این امکان را در اختیار سیاست‌گذاران و توسعه‌دهندگان قرار می‌دهد که منابع مورد نیاز را برای هر مرحله از طراحی و پیاده‌سازی الگوریتم‌های رمزنگاری مدیریت نمایند.

(جدول-۱): ماتریس تعامل ۱۳ مؤلفه پشتیبان با فرایند اصلی طراحی و پیاده‌سازی الگوریتم‌ها

(Table-1): Interaction matrix of 13 support components with the main process of designing and implementing algorithms

فرایند اصلی / مؤلفه‌ها	کاربری	مبانی	پیاده‌سازی	ارزیابی
فرهنگ	۵	۶	۵	۲
سازمان	۸	۷	۸	۸
روابط‌عمومی	۵	۴	۴	۸
منابع مالی	۷	۶	۷	۶
منابع انسانی	۸	۱۰	۱۰	۹
تحقیق و توسعه	۱۰	۸	۸	۱۰
قوانین و مقررات	۷	۴	۵	۱۰
مدیریت	۹	۷	۸	۷
فاوا	۱۰	۵	۸	۷
استاندارد	۱۰	۳	۸	۱۰
تجهیزات	۸	۶	۷	۸
زیرساخت	۷	۵	۵	۹
مواد	۷	۲	۵	۵

۴- رتبه بندی مؤلفه‌های پشتیبان با استفاده از ELECTRE III

گام ۱: ابتدا ماتریس تصمیم جدول (۱) را به‌روش نرم (رابطه ۲) بی‌مقیاس می‌کنیم.

[1] Observations

گام ۲: وزن معیارها را محاسبه می‌نماییم. برای این‌کار ابتدا ماتریس p_{ij} را برپایهٔ رابطه ۱۵ هنجار کرده تا ماتریس وزن‌دهی شانون به‌دست آید شکل (۶)

$$P_{ij}=\frac{rij}{\sum_{i=1}^{m} rij} \quad ;\forall\, i\,,j \qquad (۱۵)$$

سپس آنتروپی هر شاخص را برپایهٔ رابطه ۱۶ به‌دست می‌آوریم.

$$E_j = -k\sum_{i=1}^{m} p_{ij} \times lnp_{ij}\ ;\ i=1,2,\ldots,m \qquad (۱۶)$$

که در آن K به‌صورت رابطه ۱۷ تعریف می‌شود تا مقدار E_j را بین ۰ و ۱ نگه دارد.

$$K=\frac{1}{lnm}=\frac{1}{ln13}=0.38987125 \qquad (۱۷)$$

m تعداد شاخص‌های ماتریس تصمیم است.

E_1	E_2	E_3	E_4
0.99127	0.97297	0.9872	0.9803

در ادامه مقدار d_j (درجه انحراف) از رابطه ۱۸ محاسبه می‌شود.

$$d_j=1-E_j \qquad (۱۸)$$

d_1	d_2	d_3	d_4	d_i
0.0087	0.0270	0.012	0.019	0.0682

سپس مقدار وزن هر شاخص (W_j) برپایهٔ رابطه ۱۹ به‌دست می‌آید.

$$w_i=\frac{d_j}{\sum d_j} \qquad (۱۹)$$

W1	W2	W3	W4
0.12784	0.395949	0.18759	0.28862

(جدول-۲): ماتریس وزن‌دهی شانون

(Table-2): Shannon weighting matrix

گام / مؤلفه	کاربری	مبانی نظری	پیاده‌سازی	ارزیابی
فرهنگ	0.048	0.0822	0.0568	0.021
ساختار	0.077	0.0959	0.0909	0.083
روابط‌عمومی	0.048	0.0548	0.0454	0.073
مالی	0.068	0.0822	0.0796	0.062
منابع انسانی	0.077	0.137	0.1136	0.095
تحقیق و توسعه	0.097	0.1096	0.0909	0.104
قوانین و مقررات	0.068	0.0548	0.0568	0.104
مدیریت	0.087	0.0959	0.0909	0.073
فاوا	0.097	0.0685	0.0909	0.073
استاندارد	0.097	0.0411	0.0909	0.104
تجهیزات	0.077	0.0822	0.0796	0.083
زیرساخت	0.087	0.0685	0.0568	0.073
مواد	0.068	0.0274	0.0568	0.052

همان‌گونه که ملاحظه می‌شود، در این ماتریس بیشترین وزن مربوط به مؤلفه منابع انسانی در مبانی نظری و پیاده‌سازی الگوریتم است.

گام ۳: ماتریس بی‌مقیاس موزون v را با ضرب ماتریس هنجار در اوزان (W_j) برپایهٔ رابطه به‌دست می‌آوریم.

گام ۴: برپایهٔ روابط ۴ و ۵ و ۶ مقادیر P، q و V را محاسبه می‌کنیم.

(جدول-۳): مقادیر آستانه‌های رد، ارجحیت و بی‌تفاوتی

(Table-3): Threshold values of veto, preference and indifference

	C1	C2	C3	C4
v	0.0657	0.4407	0.1341	0.2496
p	0.0066	0.0441	0.0134	0.0250
q	0.0022	0.0147	0.0045	0.0083

گام ۵: برپایهٔ روابط ۷ و ۹ و ۱۱ ماتریس‌های هماهنگ، ناهماهنگ و اعتبار را تشکیل داده که به‌دلیل حجم زیاد، فقط ماتریس اعتبار را در جدول (۴) نشان می‌دهیم.

گام ۶: با تعیین مقادیر $\alpha=0.01$ و $\beta=0.03$ ماتریس نهایی تشکیل‌می‌شود (جدول ۵).

گام ۷: برپایهٔ ماتریس نهایی، برای هر مؤلفه، تعداد یک‌های موجود در سطر آن مؤلفه را من‌های تعداد یک‌های موجود در ستون آن می‌نماییم. عدد بزرگ‌تر به معنی اولویت بالاتر آن مؤلفه است. بر این اساس، رتبه بندی مؤلفه‌های پشتیبان به‌صورت شکل (۵) خواهد بود.

۵- اعتبارسنجی نتایج

در این بخش رتبه‌بندی مؤلفه‌های پشتیبان برپایهٔ خروجی ELECTRE III با نتایج حاصل از گزارشات شاخص جهانی امنیت سایبری[1] (GCI) سال‌های ۲۰۱۵، ۲۰۱۷ و ۲۰۱۸ که توسط ITU ارائه شده مقایسه می‌شود[57-54]. گزارش‌های GCI بر پنج شاخص تمرکز دارند که عبارتند از: "موارد حقوقی، الزامات سازمانی، موضوعات فنی، ظرفیت‌سازی و همکاری". زیر شاخص‌های مربوطه به این شرح است:

- **حقوقی:** مقررات مربوط به جرائم و امنیت فضای مجازی، مهار / محدود کردن قوانین مربوط به هرزنامه‌ها.
- **فنی:** ایجاد گروه‌های پاسخگویی حوادث رایانه‌ای[2] در سطوح ملی، دولتی و بخشی، تدوین استانداردهای فنی.
- **سازمان:** راهبری، ایجاد مراکز مسول و تعیین معیارهای امنیت فضای مجازی
- **ظرفیت‌سازی:** آگاهی عمومی، استانداردهای امنیت فضای مجازی و صدور مجوز برای متخصصان، برگزاری دوره‌های آموزشی حرفه‌ای در زمینه امنیت فضای مجازی، برنامه‌های ملی آموزش و برنامه‌های‌درسی

[1] Global Cybersecurity Index (GCI)
[2] Computer Emergency Response Team (CERT)

دانشگاهی، برنامه‌های تحقیق و توسعه امنیت فضای مجازی و تدوین سازوکارهای تشویقی.

- **همکاری:** موافقت‌نامه‌های دوجانبه و چندجانبه، مشارکت دولتی و خصوصی، مشارکت‌های بین‌سازمانی / درون‌سازمانی.

امتیازات سه کشور برتر در هر یک از حوزه‌های یادشده در جدول (۱) آورده شده‌است.

براساس شاخص‌ها و زیرشاخص‌های ارائه‌شده و امتیازات کشورهای برتر، مشخص است که پژوهش و توسعه، آموزش منابع انسانی، مدیریت، قانون و مقررات و استانداردسازی بالاترین اولویت را در ایجاد امنیت دارند. اگرچه پژوهش ما در مقایسه با گزارش‌های GCI تخصصی‌تر و مفصل‌تر است، اما این نتایج یافته‌های ما را تأیید می‌کند.

۶- نتیجه‌گیری

برای تعیین مهم‌ترین عوامل مؤثر در طراحی الگوریتم‌های رمزنگاری، ابتدا به‌روش سایبرنتیک مدل مفهومی آن رسم گردید. در این مدل چهار فرایند اصلی، راهکار / راهبرد، پشتیبان و کنترل شناسایی شدند. برپایهٔ مقالات، مستندات و گزارشات فنی معتبر در یک بازه زمانی طولانی برای فرایند اصلی ۴ گام طراحی و پیاده‌سازی و برای فرایند پشتیبان ۱۳ مؤلفه سخت‌افزاری و نرم افزاری شناسایی شد. در ادامه برپایهٔ داده‌های جمع‌آوری‌شده، میزان تأثیر هر عامل پشتیبان بر گام‌های فرایند اصلی به‌دست آمده و ماتریس تصمیم ۴×۱۳ مقداردهی شد. با توجه به تنوع مؤلفه‌ها، برای اولویت‌بندی و رتبه‌بندی آنها از روش ELECTRE III استفاده گردید. برپایهٔ خروجی حاصل از این روش، هشت مؤلفه تحقیق و توسعه، منابع انسانی، مدیریت، ساختار، فاوا، قوانین و مقررات، استاندارد و تجهیزات که دارای بالاترین اولویت هستند را در پنج سطح رتبه‌بندی نمود. بنابراین برای تدوین استراتژی رمزنگاری، مؤلفه‌های با اولویت بالا باید مورد توجه جدی قرار گرفته و منابع سخت‌افزاری و نرم‌افزاری لازم برای ارتقا آنها در نظر گرفته شود. خروجی حاصل از این روش با گزارشات ITU مقایسه و تطابق آنها با یکدیگر اثبات گردید.

پیشنهاد می‌گردد در پژوهش‌های آینده، مدل توسعه مؤلفه‌های دارای اولویت برای ارتقا دانش طراحی و پیاده‌سازی الگوریتم‌های رمزنگاری در کشور تدوین و عملیاتی شود.

۷- منابع 7-Refrece

1] L. J. Fennelly, M. Beaudry, and M. A. Perry, “Security in 2025.”

[2] Thales, “Global encryption trends study, ” Ponemon Institute Research, 2018. https://www.ncipher.com/2018/global-encryption-trendsstudy.

[3] P. Kuppuswamy and S. Q. Y. Al-Khalidi, “Hybrid encryption/decryption technique using new public key and symmetric key algorithm,” Int. J. Inf. Comput. Secur., vol. 6, no. 4, pp. 372–382, 2014, doi: 10.1504/IJICS.2014.068103.

[4] A. Vassilev, L. Feldman, and G. Witte, “ITL Bulletin for September 2018 AUTOMATED CRYPTOGRAPHIC VALIDATION (ACV) testing” no. September, pp. 1–4, 2018.

[5] NIST, “NIST Cryptographic Standards and Guidelines Development Process, ” Nist, p. 27, 2016, doi: 10.6028/NIST.IR.7977.

[6] NIST, “Report on Lightweight Cryptography March 2017 • Final Publication: https://doi.org/10.6028/NIST.IR.8114 (which links to • Information on other NIST cybersecurity publications a, ” Nist, vol. 8114, no. March, 2017.

[7] G. Alagic et al., “Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process, ” pp. 1–39, 2020, doi: 10.6028/NIST.IR.8240.

[8] V. Cerf, E. Felten, S. Lipner, B. Preneel, and E. Richey, “NIST cryptographic standards and guidelines development process: Report and recommendations of the Visiting Committee on Advanced Technology of,” 2014.

[9] I. Damaj and S. Kasbah, “An Analysis Framework for Hardware and Software Implementations with Applications from Cryptography,” 2019, doi: 10.1016/j.compeleceng.2017.06.008.

[10] S. Keller, “The Cryptographic Algorithm Validation Program, ” no. September, 2004.

[11] S. Bhat and V. Kapoor, “Secure and Efficient Data Privacy, Authentication and Integrity Schemes Using Hybrid Cryptography, ” in Advances in Intelligent Systems and Computing, 2019, vol. 870, pp. 279–285, doi: 10.1007/978-981-13-2673-8_30.

[12] P. Patil and P. Narayankar, “A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish, ” Procedia - Procedia Comput. Sci., vol. 78, pp. 617–624, 2016, doi: 10.1016/j.procs.2016.02.108.

[13] A. A. Soofi, I. Riaz, and U. Rasheed, “An Enhanced Vigenere Cipher For Data Security, ” Int. J. Sci. Technol. Res., vol. 4, no. 8, pp. 141–145, 2015.

management," Procedia - Soc. Behav. Sci., vol. 41, pp. 577–586, 2012, doi: 10.1016/j.sbspro.2012.04.070.
[27] K. T. Cho, "Multicriteria decision methods: An attempt to evaluate and unify, " Math. Comput. Model., vol. 37, no. 9–10, pp. 1099–1119, 2003, doi: 10.1016/S0895-7177(03)00122-5.
[28] P. P. Bhangale, V. P. Agrawal, and S. K. Saha, "Attribute based specification, comparison and selection of a robot, " Mech. Mach. Theory, vol. 39, no. 12 SPEC. ISS., pp. 1345–1366, 2004, doi: 10.1016/j.mechmachtheory.2004.05.020.
[29] R. V. Rao and K. K. Padmanabhan, "Selection, identification and comparison of industrial robots using digraph and matrix methods, " Robot. Comput. Integr. Manuf., vol. 22, no. 4, pp. 373–383, 2006, doi: 10.1016/j.rcim.2005.08.003.
[30] T. C. Chu and Y. C. Lin, "A fuzzy TOPSIS method for robot selection, " Int. J. Adv. Manuf. Technol., vol. 21, no. 4, pp. 284–290, 2003, doi: 10.1007 / s001700300033.
[31] T. Y. Wang, C. F. Shaw, and Y. L. Chen, "Machine selection in flexible manufacturing cell: A fuzzy multiple attribute decision-making approach, " Int. J. Prod. Res., vol. 38, no. 9, pp. 2079–2097, 2000, doi: 10.1080/002075400188519.
[32] C. Kahraman, S. Çevik, N. Y. Ates, and M. Gülbay, "Fuzzy multi-criteria evaluation of industrial robotic systems, " Comput. Ind. Eng., vol. 52, no. 4, pp. 414–433, 2007, doi: 10.1016/j.cie.2007.01.005.
[33] E. E. Karsak, "Robot selection using an integrated approach based on quality function deployment and fuzzy regression, " Int. J. Prod. Res., vol. 46, no. 3, pp. 723–738, 2008, doi: 10.1080/00207540600919571.
[34] H. S. Shih, "Incremental analysis for MCDM with an application to group TOPSIS, " Eur. J. Oper. Res., vol. 186, no. 2, pp. 720–734, 2008, doi: 10.1016/j.ejor.2007.02.012.
[35] P. Chatterjee, V. M. Athawale, and S. Chakraborty, "Selection of industrial robots using compromise ranking and outranking methods, " Robot. Comput. Integr. Manuf., vol. 26, no. 5, pp. 483–489, 2010, doi: 10.1016/j.rcim.2010.03.007.
[36] KOOPMANS and T. C., "An analysis of production as an efficient combination of activities, " Act. Anal. Prod. Alloc., 1951, Accessed: Aug. 21, 2020. [Online]. Available: https://ci.nii.ac.jp/naid/10012485947.
[37] J. M. Wilson et al., "Book Selection Evolutionary Algorithms in Management Applications, " pp. 332–334, 1997.
[38] K. B. Williams, A. Charnes, and W. W. Cooper, "Management Models and Industrial Applications of Linear Programming, " or, vol. 13, no. 3, p. 274, 1962, doi: 10.2307/3006897.
[39] B. Roy, "Classement et choix en présence de points de vue multiples, " Rev. française
[14] D. Karaoğlan Altop, A. Levi, and V. Tuzcu, "Deriving cryptographic keys from physiological signals, " Pervasive Mob. Comput., vol. 39, pp. 65–79, 2017, doi: 10.1016/j.pmcj.2016.08.004.
[15] O. Uzunkol and M. S. Kiraz, "Still wrong use of pairings in cryptography, " Appl. Math. Comput., vol. 333, pp. 467–479, 2018, doi: 10.1016/j.amc.2018.03.062.
[16] P. Pawlak and P.-N. Barmpaliou, "Politics of cybersecurity capacity building: conundrum and opportunity," J. Cyber Policy, vol. 2, no. 1, pp. 123–144, Jan. 2017, doi: 10.1080/23738871.2017.1294610.
[17] I. Mohammed and A. Musa Bade, "CYBERSECURITY CAPABILITY MATURITY MODEL FOR NETWORK SYSTEM Cyber Security Capability Maturity Model for Critical IT Infrastructure among Financial Organizations View project CYBERSECURITY CAPABILITY MATURITY MODEL FOR NETWORK SYSTEM," 2019. Accessed: Aug. 27, 2020. [Online]. Available: http://www.journalijdr.com.
[18] T. Roberts, "Cyber Security Capability Maturity Model (CMM) -Pilot. Retrieved February 18, 2016," 2014.
[19] F. Heylighen, "04. Cybernetics and second order cybernetics, " Encycl. Phys. Sci. Technol., pp. 1–24, 2001, [Online]. Available: http://www.nomads.usp.br/pesquisas/design/objetos_interativos/arquivos/restrito/heylighen_Cybernetics and Second-Order Cybernetics.pdf.
[20] A. Kappos and W. Pohlit, "A cybernetic model for radiation reactions in living cells: I. Sparsely-ionizing radiations; stationary cells, " Int. J. Radiat. Biol., vol. 22, no. 1, pp. 51–65, 1972, doi: 10.1080/09553007214550781.
[21] K. D. Jones and D. S. Kompala, "Cybernetic model of the growth dynamics of Saccharomyces cerevisiae in batch and continuous cultures, " J. Biotechnol., vol. 71, no. 1–3, pp. 105–131, 1999, doi: 10.1016/S0168-1656(99)00017-6.
[22] R. K. Pitman, "A cybernetic model of obsessive-compulsive psychopathology, " Compr. Psychiatry, vol. 28, no. 4, pp. 334–343, 1987, doi: 10.1016/0010-440X(87)90070-8.
[23] E. Wolfe and P. L. Perrewe, "A Cybernetic Model of Impression Management Processes in Organizations, " Organ. Behav. Hum. Decis. Process., vol. 69, no. 1, pp. 9–30, 1997.
[24] L. F. van Egeren, "A cybernetic model of global personality traits, " Personal. Soc. Psychol. Rev., vol. 13, no. 2, pp. 92–108, 2009, doi: 10.1177/1088868309334860.
[25] C. S. Carver, "A cybernetic model of self-attention processes, " J. Pers. Soc. Psychol., vol. 37, no. 8, pp. 1251–1281, 1979, doi: 10.1037/0022-3514.37.8.1251.
[26] M. P.A, M. H. S.M, and A. M.R, "General cybernetic model for innovation network

d’informatique Rech. opérationnelle, vol. 2, no. 8, pp. 57–75, 1968, doi: 10.1051/ro/196802v100571.
[40] M. Programming, N. P. Company, M. International, R. Received, and L. Programming, “A. X < _ b xi> _ O, ” Math. Program., vol. 1, pp. 366–375, 1971.
[41] A. M. Geoffrion, J. S. Dyer, and A. Feinberg, “Interactive Approach for Multi-Criterion Optimization, With an Application To the Operation of an Academic Department., ” Manage. Sci., vol. 19, no. 4 Part 1, pp. 357–368, 1972, doi: 10.1287/mnsc.19.4.357.
[42] P. Salminen, J. Hokkanen, and R. Lahdelma, “Comparing multicriteria methods in the context of environmental problems, ” Eur. J. Oper. Res., vol. 104, no. 3, pp. 485–496, 1998, doi: 10.1016/S0377-2217(96)00370-0.
[43] V. M. Ozernoy, “A Framework for Choosing the Most Appropriate Discrete Alternative Multiple Criteria Decision-Making Method in Decision Support Systems and Expert Systems, ” no. 1977, pp. 56–64, 1987, doi: 10.1007/978-3-642-46609-0_6.
[44] V. M. Ozernoy, “Choosing The ‘Best’ Multiple Criterlv Decision-Making Method, ” INFOR Inf. Syst. Oper. Res., vol. 30, no. 2, pp. 159–171, 1992, doi: 10.1080/03155986.1992.11732192.
[45] B. F. Hobbs, “What Can We Learn From Experiments in Multiobjective Decision Analysis?, ” IEEE Trans. Syst. Man Cybern., vol. SMC-16, no. 3, pp. 384–394, 1986, doi: 10.1109/tsmc.1986.4308970.
[46] K. Stergiou, E. C. -… and M. Biology, and undefined 1997, “The Hellenic Seas: physics, chemistry, biology and fisheries, ” pascal-francis.inist.fr, Accessed: Aug. 27, 2020. [Online]. Available: https://pascal-francis.inist.fr/vibad/index.php?action=getRecordDetail&idt=2137587.
[47] R. J. Brachman, “The Process of Knowledge Discovery in Databases: A First Sketch, ” pp. 1–11.
[48] J. Hokkanen and P. Salminen, “Choosing a solid waste management system using multicriteria decision analysis, ” Eur. J. Oper. Res., vol. 98, no. 1, pp. 19–36, 1997, doi: 10.1016/0377-2217(95)00325-8.
[49] H. Max, R. Jared, A. Don, and L. Kathleen, “Negotiation Reproduced with permission of the copyright owner. Further reproduction prohibited without permission., ” 2000.
[50] R. Store and J. Kangas, “Integrating spatial multi-criteria evaluation and expert knowledge for GIS-based habitat suitability modelling, ” Landsc. Urban Plan., vol. 55, no. 2, pp. 79–93, 2001, doi: 10.1016/S0169-2046(01)00120-7.
[51] P. Liu and X. Zhang, “Research on the supplier selection of a supply chain based on entropy weight and improved ELECTRE-III method, ” Int. J. Prod. Res., vol. 49, no. 3, pp. 637–646, Feb. 2011, doi: 10.1080/00207540903490171.
[52] S. Ottosson, Developing and Managing Innovation in a Fast Changing and Complex World. 2019.
[53] محسن رمضان یارندی, “طراحی الگوی راهبردی ایران با پیشرفت دانش و فناوری رمز در جمهوری اسلامی های رمزنگاری, ” رساله ها و پروتکل‌تأکید بر الگوریتم دکتری, ۱۳۹۹.
[53] M.Ramazan Yarandi, “Desgn of strategic model for cryptography science and technology development in Islamic Republic of Iran, emphesis on cryptography algorithms and protocols", Thesis, 1398
[54] ITU, Global Cybersecurity Index 2018. 2019.
[55] ITU, Global Cybersecurity Index (GCI) 2017. 2017.
[56] E. Wolfe et al., “A hardware implementation of Simon cryptography algorithm, ” Eur. J. Oper. Res., vol. 2, no. 3, p. 27, 2014, doi: 10.1051/ro/196802v100571.
[57] I. Peña-López, “Global cybersecurity index & cyberwellness profiles,” 2015, Accessed: Aug. 27, 2020. [Online]. Available: https://ictlogy.net/bibliography/reports/projects.php?idp=2848&lang=es.

محمد رضا عارف مدرک کارشناسی خود را در سال ۱۳۵۴ در رشته مهندسی برق از دانشکده فنی دانشگاه تهران اخذ و در همان سال با استفاده از بورس تحصیلی دانشگاه صنعتی اصفهان برای ادامه تحصیل راهی آمریکا شد و در سال ۱۳۵۵ با دریافت مدرک کارشناسی‌ارشد و در سال ۱۳۵۹ با اخذ مدرک دکترای برق مخابرات هر دو از دانشگاه استنفورد به کشور بازگشت. ایشان به‌عنوان یکی از نظریه‌پردازان مطرح جهان در نظریه اطلاعات موفق به معرفی شبکه‌ی مخابراتی معروف Aref Network شد و در راستای گسترش علم مخابرات در کشور اقدام به راه‌اندازی دکترای برق-مخابرات در دانشگاه‌های تربیت‌مدرس، صنعتی اصفهان، یزد و چند دانشگاه دیگرکرد. ترجمۀ کتاب سیستم‌های مخابراتی دیجیتال و آنالوگ که توسط ایشان انجام گرفت در سال ۶۹ به‌عنوان کتاب سال انتخاب شد.

نشانی رایانامه ایشان عبارت است از:
Aref@sharif.ac.ir

رضا رمضانی خورشید دوست در سال ۱۳۵۱ در رشته مهندسی مکانیک دانشگاه شریف مشغول به تحصیل شدند. سپس در سال ۱۳۶۳ جهت ادامه تحصیلات به آمریکا سفر کرده و مدرک کارشناسی‌ارشد خود را در دانشگاه میشیگان غربی دریافت می‌کنند. در ادامه تحصیلات به دانشگاه کیس وسترن رزرو وارد شده و مدرک دکترای مهندسی سیستم‌ها و کنترل را از این دانشگاه دریافت می‌کنند. بعد از بازگشت به ایران دکتر رمضانی خورشید دوست به‌عنوان هیئت علمی دانشگاه صنعتی امیرکبیر مشغول به فعالیت می‌شوند. مهم‌ترین زمینه‌های فعالیت ایشان در خصوص تحلیل سامانه‌های پیچیده، تحلیل سامانه‌های ساختارمند، مطالعات راهبردی، مدل‌سازی ریاضی و منطقی است.

نشانی رایانامه ایشان عبارت است از:

ramazani@aut.ac.ir

علی‌محمد نوروززاده گیل‌ملگ مدرک کارشناسی خود را در سال ۷۵ در رشته مهندسی برق – الکترونیک از دانشگاه آزاد اسلامی شرق گیلان و مدرک کارشناسی‌ارشد خود در رشته مهندسی فناوری اطلاعات گرایش امنیت اطلاعات از دانشگاه امام‌باقر (ع) و همچنین مهندسی فناوری اطلاعات گرایش شبکه‌های کامپیوتری از دانشگاه آزاد اسلامی قزوین در سال ۱۳۹۰ و مدرک دکترای تخصصی خود را در رشته مهندسی نرم‌افزار در دانشگاه آزاد اسلامی واحد تهران شمال دریافت کرد. ایشان اکنون به‌عنوان پژوهش‌گر پسا دکترا در حوزه الگوریتم‌های رمزنگاری سبک وزن در دانشگاه صنعتی شریف مشغول به فعالیت هستند. زمینه‌های پژوهشی مورد علاقه ایشان امنیت داده، امنیت شبکه‌های کامپیوتری و رمزنگاری است.

نشانی رایانامه ایشان عبارت است از:

ali.norouzzadeh@staff.sharif.edu