د کابل پوهنتون دطبیعي علومو علمي ــ څېړنیزه مجله
مجلــه علــمی- تحقیقی علــوم طبیعی پوهنتون کابل
Journal of Natural Sciences – Kabul University
e-ISSN:3078-6665 P-ISSN:3078-5561

تطبیق اصول رمزنگاری ویگنر در الفبای دری

پوهنوال منیژه سرهنگ[۱]، پوهنوال زرغونه سپیخلی[۲]

[۱،۲]دیپارتمنت ریاضیات عمومی، پوهنځی ریاضیات، پوهنتون کابل، کابل، افغانستان
ایمیل: manizha.sarhang@gmail.com

چکیده

رمزنگاری ویگنر روشی است که بر اساس نمونه‌های خاص عمل نموده و می‌تواند در الفبای دری تطبیق شود. این روش به دلیل سادگی و کاربرد آن در رمزنگاری متون، مورد توجه قرار گرفته به وسیله‌ی یک کلید متنی، متون را رمزگذاری می‌کند. دراین مقاله جدول مربعی ویگنر در الفبای دری ترتیب و با استفاده از آن جملات رمزنگاری‌شده اند و روش دوباره تبدیل به جملات رمزنگاری شده و با استفاده از کلید رمز به متن اصلی در جداول جداگانه ارایه گردیده است. هدف از این مطالعه تحلیلی و مقایسه‌ای، بررسی امکان‌پذیری و کارآمدی این روش در رمزنگاری متون دری است. با توجه به ویژگی‌های خاص ویگنر، این روش می‌تواند به‌عنوان یک شیوه‌ی مناسب برای افزایش امنیت اطلاعات مورد استفاده قرار گیرد. یافته‌های تحقیق نشان می‌دهند که استفاده از این روش می‌تواند امنیت فایل‌ها، ارتباطات اینترنتی، و احراز هویت الکترونیکی را تا حد قابل توجهی بهبود بخشد.

واژه‌های کلیدی: جریان کلیدی؛ چندالفبایی؛ خودکار؛ رمزنگاری؛ متن

Implementation of Vigener’s Cryptographic Principles in the Dari Alphabet

Manizha Sarhang[1], Zarghoona Spasely[2]

[1,2]General Mathematics Department, Mathematics Faculty, Kabul University, Kabul, Afghanistan
Email: Manizha.sarhang@gmail.com

Abstract

The Vigenère cipher is a polyalphabetic encryption method that follows specific patterns and can be adapted for the Dari alphabet. Due to its simplicity and effectiveness in text encryption, it has gained significant attention. This study applies the Vigenère cipher to Dari text by utilizing a modified Vigenère square table for encryption and decryption. Encrypted sentences are systematically converted back to their original form using a text-based key, with the process demonstrated through structured tables. The primary objective of this analytical and comparative research is to assess the feasibility and effectiveness of applying this method to Dari text encryption. Given its unique characteristics, the Vigenère cipher serves as a viable approach for enhancing information security. The findings indicate that implementing this method can significantly improve the security of files, online communications, and electronic authentication.

Keywords: Auto Key; Cryptography; Key Stream; Polyalphabetic; Text

ارجاع: سرهنگ، م. و سپیخلی، ز. (۱۴۰۳). تطبیق اصول رمزنگاری ویگنر در الفبای دری. مجله علمی- تحقیقی علوم طبیعی پوهنتون کابل، ۷(۴)، ۲۳۱-۲۴۷. https://doi.org/10.62810/jns.v7i4

مقدمه

کلمه‌ی رمزنگاری برگرفته شده از لغات یونانی به معنی محرمانه نوشتن متون است. رمزنگاری علم کودها و رمزهاست. رمزنگاری یک هنر قدیمی بوده که قرن‌ها به منظور محافظت از پیام‌هایی‌که بین فرماندهان، جاسوسان و دیگران رد و بدل شده است، استفاده گردیده است (Swenson, 2008; Preneel, 2010).

هنگامی که با امنیت معلومات سروکار داشته باشیم، نیاز به اثبات هویت فرستنده و گیرنده‌ی پیام نیز داریم و در ضمن باید از عدم تغییر محتوای پیام مطمئن باشیم. این سه موضوع یعنی، محرمانگی، تصدیق هویت و جامعیت در قلب امنیت ارتباطات معلوماتی مُدرن قرار دارند و می‌توانند در رمزنگاری از آن‌ها استفاده گردد. روشی که تأمین‌کننده این مسأله باشد (رمزنگاری) نام دارد(کریمی، ۱۴۰۰ ; تورج، ۱۴۰۰ ;Klima, 2013).

رمزنگاری روش ویگنر که با الفبای نورمال و رایجی همراه است، بر علاوه جدول مربعی از حساب پیمانه (مود) نیز استفاده می‌گردد که خاصیت جابه‌جایی دارد (یوسف راد، ۱۳۹۸ ;Damico, 2009). رمز ویگنر در حقیقت در سال **۱۵۵۳** توسط فردی به نام جیوان باتیستا بلاسو تعریف شده بود؛ اما ویگنر[1] (**۱۵۲۳-۱۵۹۶**) در سال **۱۵۸۵** مقاله‌یی منتشر کرد که این رمز را در آن تعریف کرد. از آن رو، این رمز به نام رمز ویگنر معروف است (Shparlinski, 2003; Paar, 2010; Albrecht, 2001).

این رمز در سال **۱۸۶۸** توسط چارلز داگسن[2] "غیرقابل نفود" نامیده شد. در سال**۱۹۱۷** نشریه ساینتفیک امریکن[3] اعلام داشت که این رمز غیرقابل تفسیر است. چندین سال بعد فردی به نام کاسیسکی روشی برای شکستن رمز ابداع کرد که به تنهایی کافی نبود. گفته می‌شود رمزشکنان با تجربه قرن۱۶- ام نیز از روش کاسیسکی برای شکستن رمز ویگنر استفاده می‌کردند(Klaus, 2003; Rosulek, 2021). اما تلاش‌های انجام شده جهت شکستن آن سه قرن به طول انجامید که نشان‌گر ساختار غیرقابل حدس آن را ارایه می‌دارد. برای رمزگذاری متن با استفاده از این روش، ابتدا باید یک کلمه یا عبارت کلیدی انتخاب کنیم. سپس، این کلمه کلیدی را بارها و بارها تا زمانی که اندازه‌ی طول آن برابر با اندازه طول متن اصلی شود، تکرار کنیم. به این روند، جریان کلیدی می‌گویند (Philippe Aumasson, 2017; Katz, 2015; Naser, 2021; Talbot, 2005).

---

[1] Blaise de Vigenère
[2] Charles Lutwidge Dodgson
[3] Scientific American

اکنون برای هرحرف از متن اصلی، حرف مربوطه را از جریان کلیدی دریافت کرده و آن را در ستون‌های جدول ویگنر پیدا می‌کنیم. سپس حرف اصلی را در ردیف‌ها می‌یابیم. جایی که این دو خط در جدول متقاطع هستند حرف رمزگذاری متن مورد استفاده است. برای بیان موضوع در یک جمله این روش به خوبی شرح داده شده است(Koblitz, 1998; Stinson & Paterson, 2019). چنانچه ذکرشد که برای رمزنگاری یک متن اصلی با استفاده از روش ویگنر، نخست باید جدول مربعی از حروف را ترتیب نماییم بعداً یک کلمه، یک عبارت یا یک متن مورد نظر را که می‌خواهیم رمز نماییم انتخاب و سپس، یک کلمه کلیدی را برای رمز، مد نظر گیریم و این کلمه کلیدی را بارها و بارها تا زمانی که اندازه‌ی طول آن برابر با اندازه‌ی طول متن اصلی شود، تکرار بنویسیم که به این روند، جریان کلیدی هم گویند. اکنون تقاطع برای هر حرف از متن اصلی و کلمه کلیدی را در جدول مربعی الفبای مورد نظر پیدا می‌کنیم. طوری که حروف کلیدی را در سطر اول و حروف متن را در ستون اول جدول مربعی الفبای مورد نظر از جریان کلیدی دریافت می‌نماییم (حیدری، ۱۳۹۹;Brassard, 1988) هرچند رمزنگاری به این روش نظر به رمزنگاری‌های آن عصر، نسبتاً امن‌تر بوده؛ اما هنوز هم آسیب‌پذیر می‌باشد. زیرا هر قدر کلمه کلیدی انتخابی، طولانی‌تر باشد، رمزنگاری امنیت بیشتری خواهد داشت (Goldreich, 1999; Thomas et al ,2009). نخست جدول مربعی از حروف الفبای دری را ترتیب و بعداً بااستفاده از روش ویگنر می‌توان یک جمله را رمز نمود. چون حروف الفبای دری۳۳ حرف است، پس جدول مربعی از ۳۳ حروف دری را ترتیب می‌دهیم.

جدول۱: ترتیب جدول مربعی حروف الفبای دری با استفاده از جدول مربعی ویگنر (نویسندگان،۱۴۰۳)

	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی
آ	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی
ا	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ
ب	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا
پ	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب
ت	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ
ث	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ	ت
ج	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ	ت	ث
چ	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ	ت	ث	ج
ح	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ	ت	ث	ج	چ
خ	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ	ت	ث	ج	چ	ح
د	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ
ذ	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د
ر	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ
ز	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر
ژ	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز
س	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ
ش	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س
ص	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش
ض	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص
ط	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض

ظ	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط
ع	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ
غ	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع
ف	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ
ق	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف
ک	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق
گ	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک
ل	ل	م	ن	و	ه	ی	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ
م	م	ن	و	ه	ی	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل
ن	ن	و	ه	ی	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م
و	و	ه	ی	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن
ه	ه	ی	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و
ی	ی	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه

حالادر جدول(۲) -ام می‌خواهیم جمله(بهشت زیرپای مادران است) را با استفاده از کلید (علم) رمزگذاری نماییم. پس هر حرف متن را جدا- جدا نوشته و حروف کلید را به آن تقسیم می‌کنیم.

جدول۲: تقسیم حروف کلید روی حروف متن جمله مدنظر (نویسندگان، ۱۴۰۳)

متن	ب	ه	ش	ت	ز	ی	ر	پ	ا	ی	م	ا	د	ر	ا	ن	ا	س	ت
کلید	ع	ل	م	ع	ل	م	ع	ل	م	ع	ل	م	ع	ل	م	ع	ل	م	ع

حالانقاط تقاطع حروف متن اصلی را با استفاده ازحروف کلید، نظر به جدول مربعی ویگنر در حروف الفبای دری همانند جدول(۳) -ام به دست می‌آوریم، قسمی‌که نقطه تقاطع حرف اول متن مورد رمز را در ستون (از بالا به پایین) و حرف اول کلید را در سطر(از طرف راست به چپ) پیدامی‌کنیم.

جدول۳: تقاطع حرف اول کلید(درسطر) با حرف اول متن جمله مورد نظر(در ستون)(نویسندگان، ۱۴۰۳)

	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع
آ	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع
ا	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ
ب	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف

این مراحل را مجدداً تکرار می کنیم. همه نقاط تقاطع حروف متن رمز شده را درجدول(٤)-ام ترتیب می‌نماییم.

جدول٤: تقاطع حرف دوم کلید با حرف دوم متن جمله مورد نظر (نویسندگان، ۱۴۰۳)

	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل
آ	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل
ا	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م
ب	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن
پ	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و
ت	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه
ث	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی
ج	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ
چ	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا
ح	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب

خ	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ
د	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ	ت
ذ	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ	ت	ث
ر	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ	ت	ث	ج
ز	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ	ت	ث	ج	چ
ژ	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ	ت	ث	ج	چ	ح
س	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ
ش	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د
ص	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ
ض	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر
ط	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز
ظ	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ
ع	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س
غ	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش
ف	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص
ق	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض
ک	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط
گ	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ
ل	ل	م	ن	و	ه	ی	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع
م	م	ن	و	ه	ی	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ
ن	ن	و	ه	ی	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف
و	و	ه	ی	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق
ه	ه	ی	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک

ک = ل ∩ ه

جدول ۵: تقاطع حرف سوم کلید با حرف سوم متن جمله مورد نظر (نویسندگان، ۱۴۰۳)

	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م
آ	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م
ا	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن
ب	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و
پ	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه
ت	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی
ث	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ
ج	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا
چ	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب
ح	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ
خ	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ	ت
د	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ	ت	ث
ذ	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ	ت	ث	ج
ر	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ	ت	ث	ج	چ
ز	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ	ت	ث	ج	چ	ح
ژ	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ
س	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د
ش	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ

ذ = م ∩ ش

جدول۶: تقاطع حرف اول کلید با حرف چهارم متن جمله مورد نظر (نویسندگان، ۱۴۰۳)

	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع
آ	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع
ا	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ
ب	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف
پ	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق
ت	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک

ک = ع ∩ ت

جدول ۶ ترتیب جمع آوری تقاطع حروف متن اصلی وحروف کلید انتخابی، را از جدول حروف الفبای دری، بیان می‌کند.

جدول ۷: جمع آوری‌تقاطع حروف کلید با حروف متن جمله مورد نظر (نویسندگان، ۱۴۰۳)

متن	**ب**	**ه**	**ش**	**ت**	**ز**	**ی**	**ر**	**پ**	**ا**	**ی**	**م**	**ا**	**د**	**ر**	**ا**	**ن**	**ا**	**س**	**ت**
کلید	**ع**	**ل**	**م**	**ع**	**ل**	**م**	**ع**	**ل**	**م**	**ع**	**ل**	**م**	**ع**	**ل**	**م**	**ع**	**ل**	**م**	**ع**
رمز	**ف**	**ک**	**ذ**	**ک**	**چ**	**ل**	**ا**	**و**	**ل**	**ظ**	**غ**	**ل**	**ه**	**ح**	**ل**	**ص**	**ل**	**د**	**ک**

متن اصلی: بهشت زیرپای مادران است.

کلید: علم

متن رمزنگاری شده: فکذ کچلا ولظغله حلصلدک.

با استفاده از روش رمزنگاری ویگنر متن اصلی را که (بهشت زیر پای مادران است) تبدیل به متن رمز شده‌یی (فکذ کچلا ولظغله حلصلدک) شد که به هیچ صورت قابل فهم برای افراد غیر مجاز نبوده و نیست.

اگر خواستیم که متن رمزنگاری شده را به متن اصلی دوباره تبدیل نماییم پس جدول(۷) را در نظر می‌گیریم طوری‌که، حروف کلید و رمز را روی هم تقسیم می نماییم.

جدول۸: تقسیم حروف کلید روی رمز به دست آمده (نویسندگان، ۱۴۰۳)

کلید	ع	ل	م	ع	ل	م	ع	ل	م	ع	ل	م	ع	ل	م	ع	ل	م	ع
رمز	ف	ک	ذ	ک	چ	ل	ا	و	ل	ظ	غ	ل	ه	ح	ل	ص	ل	د	ک

حروف کلید را در سطر در نظر گرفته و به استقامت همان حرف کلید به شکل ستونی حرف رمز را می‌یابیم که تقاطع به کدام حرف در جدول الفبای دری می‌کند که همانا هر یک حرف، حرفی از حروف متن اصلی می‌باشد.

<u>در مرحله اول:</u> حرف اول کلید را در جدول دریافت کرده و به شکل ستونی حرف رمز را پیدا می‌کنیم، حرفی که در سطر به استقامت حرف رمز است، عبارت از حرف اول متن اصلی می‌باشد.

جداول۹: دریافت حرف اول کلید به شکل ستونی باحرف اول رمز به دست آمده. (نویسندگان،۱۴۰۳) ↓

	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع
آ	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع
ا	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ
ب	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف

→ → → → → → → → → → → →

در مرحله دوم و مراحل بعدی روش را به عین ترتیب انجام می‌دهیم.

جدول۱۰: دریافت حرف دوم کلید به شکل ستونی باحرف دوم رمز به دست آمده (نویسندگان،۱۴۰۳)

	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل
آ	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل
ا	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م
ب	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن
پ	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و
ت	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه
ث	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی
ج	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ
چ	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا
ح	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب
خ	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ
د	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ	ت
ذ	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ	ت	ث
ر	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ	ت	ث	ج
ز	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ	ت	ث	ج	چ

ژ	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ	ت	ث	ج	چ	ح
س	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ
ش	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د
ص	ص	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ
ض	ض	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر
ط	ط	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز
ظ	ظ	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ
ع	ع	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س
غ	غ	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش
ف	ف	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص
ق	ق	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض
ک	ک	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط
گ	گ	ل	م	ن	و	ه	ی	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ
ل	ل	م	ن	و	ه	ی	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع
م	م	ن	و	ه	ی	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ
ن	ن	و	ه	ی	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف
و	و	ه	ی	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق
ه	ه	ی	آ	ا	ب	پ	ت	ث	ج	چ	ح	خ	د	ذ	ر	ز	ژ	س	ش	ص	ض	ط	ظ	ع	غ	ف	ق	ک

باالاخره با تطبیق نمودن این روش همه حروف متن اصلی را می‌یابیم.

جداول۱۱: ترتیب دریافت همه حروف کلید به شکل ستونی باهمه ی حروف رمزبه دست آمده. (نویسندگان،۱۴۰۳)

کلید	ع	ل	م	ع	ل	م	ع	ل	م	ع	ل	م	ع	ل	م	ع	ل	م	ع
رمز	ف	ک	ذ	ک	چ	ل	ا	و	ل	ظ	غ	ل	ه	ح	ل	ص	ل	د	ک
متن	ب	ه	ش	ت	ز	ی	ر	پ	ا	ی	م	ا	د	ر	ا	ن	ا	س	ت

کلید: علم

متن رمزنگاری شده: فکذ کچلا ولظغله حلصلدک.

متن اصلی: بهشت زیر پای مادران است.

یافته‌ها

روش رمزنگاری ویگنر به‌راحتی برای الفبای دری و سایر زبان‌ها قابل تطبیق است و امکان رمزگذاری معلومات محرمانه را در قالب متن یا داده‌های اینترنتی فراهم می‌کند. این روش با جابه‌جایی حروف بر اساس یک کلید رمز، امنیت اطلاعات را افزایش داده و از دسترسی غیرمجاز جلوگیری می‌کند. در مقایسه با سایر روش‌های رمزنگاری، این روش به دلیل سادگی و انعطاف‌پذیری، گزینه‌ای مناسب برای رمزگذاری متون دری محسوب می‌شود. بااین‌حال، مدیریت کلید در این روش چالش‌برانگیز بوده و امنیت آن به طول کلید بستگی دارد؛ به‌طوری‌که برای جلوگیری از شکست رمز، طول کلید باید حداقل برابر با طول متن باشد.

یکی از اصول کلیدی در رمزنگاری ویگنر، استفاده از تکرار حروف در تحلیل آماری فریکونسی است که مشابه سایر روش‌های چندالفبایی به‌کار گرفته می‌شود. امنیت این روش درصورتی حفظ می‌شود که کلید مورد استفاده به‌اندازه‌ی کافی طولانی باشد، زیرا مهم‌ترین ضعف آن، تکرار کلید است. در صورتی که طول کلید قابل حدس باشد، رمزنگاری ویگنر می‌تواند مانند رمزنگاری سزار مورد حمله قرار گیرد. در چنین شرایطی، با استفاده از تحلیل فریکونسی حروف و روش‌هایی مانند کاسیسکی و آزمون فریدمن، امکان شکستن سیستم رمز و تعیین طول کلید فراهم می‌شود.

نتیجه‌گیری

نتایج این تحقیق نشان می‌دهد که رمزنگاری ویگنر با استفاده از یک کلمه‌ی کلیدی و یک جدول رمزنگاری، متون را به‌طور مؤثر رمزگذاری می‌کند. این روش که توسط رمزنگار فرانسوی ویگنر ابداع شده، متن را به‌صورت سطری و بدون فضای اضافی رمزگذاری می‌کند. بررسی‌ها نشان می‌دهد که این روش به دلیل ویژگی‌های خاص خود، یکی از راهکارهای مناسب برای حفظ امنیت اطلاعات است.

بااین‌حال، یکی از چالش‌های این روش، وابستگی آن به طول کلید است؛ چنانچه کلید کوتاه‌تر از متن اصلی باشد، امکان رمزگشایی آن افزایش می‌یابد. بنابراین، برای بهبود امنیت، استفاده از کلیدهای طولانی‌تر توصیه می‌شود. در مجموع، یافته‌های این تحقیق نشان می‌دهد که با بهره‌گیری از روش ویگنر، می‌توان امنیت فایل‌ها، اطلاعات حساس، ارتباطات اینترنتی و احراز هویت الکترونیکی را به میزان قابل توجهی افزایش داد.

منابع

تورج، ا. (۱۴۰۰). *اصول و مفاهیم رمزنگاری*. انتشارات نشر بید.

حیدری، م. خ. (۱۳۹۹). *نظریه تطابق*. مطبعه پوهنتون کابل، افغانستان.

کریمی، س. س. (۱۴۰۰). *آموزش اصول و مفاهیم تست نفوذ*. انتشارات سها. تهران.

یوسفی راد، ا. فروزان، ب. شکری، م. (۱۳۹۸). *رمزنگاری*، موسسه فرهنگی هنری دیباگران تهران.

Beutelspacher, A., & Schwenk. (2001). *Moderne Verfahren der Kryptographie*. Vieweg, Braunschweig. ISBN: 3704016632.

Brassard, G. (1988). *Modern Cryptology*. Lecture Notes in Computer Science. Springer-Verlag, Berlin. ISBN: 10- 0387968423.

Broemeling, L. D. (2011). *An Account of Early Statistical Inference in Arab Cryptology*. 2297-0584The American Statistician,65(4).

Bruen, A. A., & Forcinito, M.A. (2004). *CRYPTOLOGY INFORMATION THEORY AND ERROR CORRECTION*: A Handbook for the 21 st Century, John Wiley & Sons Inc, New Jersey. ISBN 0-471-65317-9.

Delfs, H, & Knebl, H. (2015). *Principles and Applications (Information Security and Cryptography)* 3rd ed. ISBN-10 3662479737.

Shparlinski, I. (2003). *Cryptographic Applications of Analytic Number Theory*. Birkhäuser-Verlag, Basel. ISBN: 2297-0584.

Talbot, J., & Welsh, D. (2005). *Complexity and Cryptography*. Cambridge University Press. ISBN-13 978-0-511-14070-9.

Katz, J. (2015). *Introduction to Modern Cryptography*. Taylor & Francis Gtoup. ISBN-13: 978-1-4665-7027-6.

Lennon, B. (2018). *Philology, Security, Authentication*. Harvard University Press, Cambridge. DOI:10.1086/712124 .

Naser, S. M. (2021). CRYPTOGRAPHY. Department of Mathematics, Bangladesh University of Engineering and Technology, *International Journal of Mathematics and Statistics Studies*. https://papers.ssrn.com

Klima, R, E, & Sigmon, N, P. (2013). Cryptology. Appalachian State University Boone, North Carolina, USA. By Taylor & Francis Group. ISBN: 13: 798-1-4665-6904-1.

Koblitz, N. (1998). *Algebraic Aspects of Cryptography*. Springer-Verlag, Berlin.

Goldreich, O. (1999). *Modern Cryptography*, Springer-Verlag, Berlin.

Paar, C., & Pelzl, J. (2010). Understanding Cryptograph: A Textbook for Students and Practitioners, Springer, Hedelberg Dordrecht London New York. DOIhttps://doi.org/10.1007/978-3-642-04101-3.

Philippe Aumasson, J. (2017). *Serious Cryptography*. No Starch Press. ISBN-10 1593278268**.**

Preneel, B. (2010). *Understanding Cryptography*. Springer-Verlag Berlin Heidelberg. ISBN 978-3-642-04100-6.

Rosulek, M. (2021). *The Joy Cryptography.* School of Electrical Engineering & Computer Science Oregon State University, Corvallis, Oregon, USA.

Schmeh, K. (2003). *Cryptography and Public Key Infrastructure on the Internet*. John Wiley, New Yor. ISBN: 978-0-470-86248-3.

Stinson, D R., & Paterson, M B. (2019). *Cryptography Theory and Practice*. Taylor & Francis Group, LLC. ISBN-13: 978-1-1381-9701-5.

Swenson, C. (2008). *Modern Cryptanalysis*. Wiley Publishing, Indianapolis. ISBN-10 047013593X.

Thomas, W., & Pantelimon, S. (2009). *Cryptographic BooleanFunctions and Applications*. Academic Press. ISBN: 978-0-1237-4890-4.