शोध पत्र / Research Paper

# कूटलेखन के लिए आलेख सिद्धांत और चेबिशेव बहुपदों का उपयोग करते हुए एक नवीन गूढ़ालेखी ढाँचा

## A Novel Cryptographic Framework for Encryption Employing Graph Theory and Chebyshev Polynomials


**मोहम्मद आमिर[1], बृजेश शुक्ल[2] एवं इष्ट विभु[2*]**

**Mohammad Amir[1*], Brijesh Shukla[2] and Isht Vibhu[2*]**

[1]Department of Mathematics, Yuveraj Dutta Postgraduate College, Lakhimpur Kheri, U.P., India-262701

[2]Department of Physics, Yuveraj Dutta Postgraduate College, Lakhimpur Kheri, U.P., India-262701

aamir329@gmail.com, brijeshshukla17@gmail.com, ishtvibhu@gmail.com

*Corresponding author



https://doi.org/10.5281/zenodo.19667322



**सारांश**

इस शोध पत्र में, ग्राफ सिद्धांत की गणितीय जटिलता और चेबिशेव बहुपदों के विश्रंखल–अनियमित (chaotic) गुणों के समन्वय से एक नवीन एनक्रिप्शन तकनीक प्रस्तुत की गई है। यह सम्भावना है कि यह तकनीक पारंपरिक क्रिप्टोग्राफिक योजनाओं जैसे आरएसए, एलगामल, श्नोर, और डीएसए का एक सशक्त और उन्नत विकल्प हो सकती है। पारंपरिक एल्गोरिदम जहां मुख्य रूप से पूर्णांक गुणनखंडन या विवक्ति लघुगणक जैसे संख्या–सिद्धांत संबंधी समस्याओं की कम्प्यूटेशनल कठिनाई पर निर्भर करते हैं, वहीं पर प्रस्तुत नवीन तकनीक ग्राफ संरचनाओं की जटिलता और चेबिशेव बहुपदों की अभिकलनात्मक (computational) दक्षता पर आधारित है।

इस कूटलेखन प्रणाली में ग्राफीय निरूपण, जैसे आसन्नता आव्यूह (adjacency matrix) और स्पेक्ट्रमी गुणधर्मों को क्रिप्टोग्राफिक कुंजी के रूप में उपयोग किया गया है, और चेबिशेव बहुपदों का उपयोग उनके पुनरावर्ती और विश्रंखल–अनियमित (chaotic) गुणधर्मों के कारण कूटलेखन (encryption) और विकूटन (decryption) के लिए किया गया है। इन तकनीकों के संयोजन से यह पद्धति पारंपरिक क्रिप्टोएनालिटिक हमलों के विरुद्ध उच्च स्तर की सुरक्षा, प्रतिरोध, और आधुनिक क्रिप्टोग्राफिक आवश्यकताओं यथा आसान और वस्तुसंजाल (IoT) अनुप्रयोगों के लिए उपयुक्त अभिकलनात्मक दक्षता प्रदान करती है।

**Abstract**

In this paper, we propose a novel encryption technique that integrates the mathematical robustness of graph theory with the chaotic properties of Chebyshev polynomials. It is possible that this technique may prove to be an alternative to traditional cryptographic schemes such as RSA, ElGamal, Schnorr, and DSA. While these classical algorithms rely heavily on the computational hardness of number-theoretic problems like integer factorization or discrete logarithms, the approach presented here leverages the structural complexity of graphs and the computational efficiency of Chebyshev polynomials.

The encryption system utilizes graph representations, such as adjacency matrices and spectral properties, as cryptographic keys, while Chebyshev polynomials provide the foundation for encryption

and decryption through their recursive and chaotic nature. By combining these techniques, the proposed method achieves a high degree of security, resilience against conventional cryptanalytic attacks, and computational efficiency suitable for modern cryptographic demands, including lightweight and IoT applications.

**मुख्यशब्दः** गूढ़ालेखी, आलेख सिद्धांत, चेबिशेव बहुपद, आसन्नता आव्यूह, स्पेक्ट्रमी गुणधर्म, अभिकलनात्मक दक्षता, विश्रृंखल–अनियमित निकाय।

**Key words:** Cryptography, Graph Theory, Chebyshev Polynomials, Adjacency Matrices, Spectral Properties, Computational Efficiency, Chaotic Systems.

## परिचय

जैसे–जैसे डिजिटल संचार अभूतपूर्व गति से बढ़ रहा है, सुरक्षित और अभिकलनात्मक (computational) रूप से कुशल एन्क्रिप्शन तकनीकों की मांग पहले से कहीं अधिक महत्वपूर्ण हो गई है [1]। विविध अनुप्रयोगों में डेटा की गोपनीयता और समग्रता की रक्षा की यह तात्कालिक आवश्यकता (urgency), आधुनिक गूढ़ालेखी विधियों की परिष्कृत गणितीय संरचनाओं (sophisticated mathematical structures) पर निर्भरता को रेखांकित करती है [1]। सुरक्षा और प्रदर्शन (performance) की उभरती हुई चुनौतियों के निपटान मे अभिनव समाधान की आवश्यकता कूटलेखन की निरंतर प्रगति को प्रेरित करती है।

गूढ़ालेखी तकनीकों का विकास सुरक्षा, दक्षता और अनुकूलनशीलता के बीच संतुलन स्थापित करने के लिए निरंतर जारी खोज पर प्रकाश डालता है। प्रारंभिक विधियाँ, जैसे कि 1976 में प्रस्तुत डिफी–हेलमैन कुंजी विनिमय [2], असुरक्षित माध्यमों पर सुरक्षित कुंजी साझा करने की सुविधा प्रदान करती थीं, तथापि विवित्त लघुगुणक (discrete logarithms) पर इसकी निर्भरता इसे उदीयमान क्वांटम खतरों (quantum threats ) से असुरक्षित रखती है [3]। इसी तरह मजबूत सुरक्षा प्रदान करने के लिए 1978 मे पूर्णांकों के गुणनखंडन (integer factorization) पर आधारित, RSA [4] प्रस्तुत की गई, परंतु इसके लिए उच्च संगणनात्मक संसाधनों की आवश्यकता होती है, जो हल्के सिस्टम में इसके उपयोग को सीमित कर देती है [5]। विविक्त लघुगणकों पर आधारित एलगामल [6] और श्नॉर [7] हस्ताक्षर योजनाएं दक्षता प्रदान करती हैं, किंतु ये भी विस्तारशीलता (scalability) और कुंजी आकार की चुनौतियों का सामना करती हैं [1]। 1991 में मानकीकृत डिजिटल सिग्नेचर एल्गोरिथ्म (DSA) [8], डिजिटल हस्ताक्षर के प्रदर्शन को बेहतर बनाता है, लेकिन यह भी अपने पूर्ववर्तियों की तरह क्वांटम खतरों के प्रति असुरक्षित है [9]। हाल के नवाचार, जैसे कि चेबिशेव बहुपदों (Chebyshev polynomials) पर आधारित अराजकता–आधारित कूटलेखन [10], अप्रत्याशितता और हल्के संगणन की क्षमता प्रदान करते हैं, यद्यपि इनकी व्यावहारिक शक्यता अभी परीक्षण की स्थिति में है [11]। पोस्ट–क्वांटम दृष्टिकोण [12] भविष्य के खतरों का मुकाबला करने के लिए उच्च सुरक्षा प्रदान करते हैं, लेकिन इसकी कीमत बढ़ी हुई जटिलता के रूप में चुकानी पड़ती है [13]। वर्तमान कमियों को दूर करने मे इन विधियों की सामर्थ्य और सीमाएं, उपयुक्त अभिनव संकर (hybrid) समाधानों की आवश्यकता को स्पष्ट करती हैं।

इस आवश्यकता को पूरा करने हेतु, यहाँ आलेख सिद्धांत [14] की संरचनात्मक जटिलता को उन्नत कुंजी विनिमय तंत्रों तथा चेबिशेव बहुपदों [15] की अराजक गतिशीलता के साथ एकीकृत करते हुए नवोन्मेषी कूटन तकनीक प्रस्तावित की गई है। इस विधि में एक पूर्ण आलेख से भारित आसन्नता आव्यूह (weighted adjacency matrix) का निर्माण किया जाता है, जिसमें, इस प्रकार ठोस गूढ़ालेखी आधार के रूप में आलेख की जटिलता का लाभ लेते हुए, संदेश को एक बाह्य हैमिल्टोनियन पथ पर घड़ी की दिशा में संचरण करते हुए एन्कोड किया जाता है [16]। एक साझा कुंजी से इस आव्यूह को गुणा करके सुरक्षा को और अधिक बढ़ाया जाता है, कुंजी का विनिमय डिफी–हेलमैन प्रेरित प्रोटोकॉल [2] के माध्यम से किया जाता है, जो प्रत्यक्ष संचरण के बिना सुरक्षित कुंजी स्थापना सुनिश्चित करता है [12]। प्राप्त आव्यूह का चेबिशेव बहुपदों [10]

द्वारा संवर्धित आरएसए–प्रेरित स्कीम [4] का उपयोग करते हुए कूटन किया जाता है। चेबिशेव बहुपदों के पुनरावर्ती एवं अराजक गुणधर्म [17] अनाधिकृत विकूटन को संगणनात्मक रूप से असंभव बना देते हैं [1]।

यह दृष्टिकोण पारंपरिक योजनाओं जैसे कि एलगामल [6], डीएसए [8], और श्नॉर [7] से भिन्न है। ये पारंपरिक योजनाएं केवल विवित्त लघुगणकों [18] या पूर्णांकों के गुणनखंडन पर आधारित, आरएसए [4] पर निर्भर होती हैं। प्रस्तावित विधि इन दोनों कठिन समस्याओं–विवित्त लघुगणक द्वारा कुंजी विनिमय [2] और एन्क्रिप्शन के लिए गुणनखंडन के जरिए कूटन [4]–के मेल से एक द्विस्तरीय रक्षा तंत्र (dual–layered defence) स्थापित करती है। यह द्विस्तरीय सुरक्षा प्रणाली क्रिप्टोविश्लेषण (cryptanalysis) के प्रति प्रतिरोध को सार्थक रूप से बढ़ा देती है [12]।यह शोध पत्र एक सशक्त और विस्तारशील (scalable) क्रिप्टोसिस्टम के लिए आलेख सिद्धांत [14], कुंजी विनिमय [2], और चेबिशेव–संवर्धित आरएसए कूटन [17] के संश्लिष्ट दृष्टिकोण का उपयोग कर कई प्रस्तावित विधि का विवरण प्रस्तुत करता है। यह प्रणाली मजबूत सुरक्षा के साथ–साथ कुशल संगणन भी प्रदान करती है, जिससे यह हल्के IoT उपकरणों से लेकर उच्च–जोखिम वाली डिजिटल संचार प्रणालियों [19] तक के अनुप्रयोगों के लिए आदर्श बन जाती है।

## प्रस्तावित एन्क्रिप्शन तकनीकों की गणितीय आधारशिला

आव्यूह – आधारित कुंजी विनिमय, आलेख सिद्धांत, चेबिशेव बहुपद, और एक RSA–जैसे दृष्टिकोण को एकीकृत करते हुए यह अनुभाग प्रस्तावित कूटन योजनाओं के गणितीय आधार की रूपरेखा प्रस्तुत करता है। सामूहिक रूप से ये सभी घटक – विवित्त लघुगणकों की कठिनता, आलेख की संरचनात्मक जटिलता, बहुपद पुनरावृत्तियों की अराजक प्रकृति, और RSA–जैसे सिस्टम में गुणनखंडन की कठिनाई [1] मिलकर एक मजबूत गूढ़ालेखी ढांचा बनाते हैं। निम्नलिखित चार उपखंडों में प्रत्येक गणितीय आधार का विवरण दिया गया है:

A. सुरक्षित कुंजी साझाकरण के लिए डिफी–हेलमैन कुंजी विनिमय का एक आव्यूह –आधारित विस्तार,

B. संदेश निरूपण के लिए आलेख – सिद्धांत पर आधारित एक मॉडल,

C. चेबिशेव बहुपदों के गुणधर्म, जो कूटन की अप्रत्याशितता (encryption unpredictability) को बढ़ाते हैं, और

D. कूटन और विकूटन के लिए चेबिशेव बहुपदों का उपयोग करने वाली एक प्रस्तावित RSA–प्रेरित योजना।

### A. मैट्रिक्स–आधारित डिफी–हेलमैन कुंजी विनिमय

प्रतिष्ठित डिफी–हेलमैन कुंजी विनिमय [2] – जो गूढ़ालेखी नवाचार की आधारशिला मानी जाती है यह विधि डिफी–हेलमैन कुंजी विनिमय [2] के स्केलर (scalar) ढांचे को आव्यूह के क्षेत्र में विस्तारित करके परिष्कृत करती है, जिसमें घातांक (exponents) केवल धनात्मक पूर्णांकों तक सीमित होते हैं। यह विधि दो पक्षों–परंपरागत रूप से एलिस और बॉब–को परिमित क्षेत्र (finite field) में मापांक अंकगणित (modular arithmetic) की सटीकता का उपयोग करके एक साझा गुप्त आव्यूह स्थापित करने की अनुमति देती है। इस अनुकूलन की नवीनता केवल इसके सैद्धांतिक कौशल में ही नहीं, बल्कि इसकी व्यावहारिक प्रभावशीलता में भी निहित है: यह एन्क्रिप्टेड संचार से लेकर नेटवर्क प्रणालियों की सुरक्षा तक के अनुप्रयोगों के लिए सुरक्षित कुंजी व्युत्पत्ति को संभव बनाता है, और क्रिप्टोग्राफरों के लिए एक बहुपयोगी उपकरण प्रदान करता है [1, 19]।

#### A.1 सार्वजनिक प्राचल

• आकार (n×n) का लोकसम्मत (public agreed) आधार आव्यूह B एक बड़े अभाज्य संख्या r के मापांक परिमित क्षेत्र से चुना जाता है यह विनिमय की आधार संरचना के रूप में कार्य करता है।

• एक बड़ी अभाज्य संख्या r मापांक संक्रियाओं (modular operations) को नियंत्रित करती है, जिसका

परिमाण व्यापक आक्रमणों के विरुद्ध एक शक्तिशाली अवरोध सुनिश्चित करता है।

### A.2 कुंजी विनिमय की चरणबद्ध प्रक्रिया

#### A.2.1 निजी कुंजी का चयनः

एलिस एक गुप्त पूर्णांक a चुनती है, जिसे वह किसी से साझा नहीं करती। इसी प्रकार, बॉब एक गुप्त पूर्णांक b चुनता है, जिसे केवल वही जानता है।

#### A.2.2 सार्वजनिक कुंजी की गणनाः

• एलिस मैट्रिक्स A की गणना किस प्रकार करती है:

$A = B^a \pmod r$

फिर वह मैट्रिक्स A को बॉब को भेजती है।

• बॉब अपनी सार्वजनिक मैट्रिक्स की गणना निम्न प्रकार करताः

$C = B^b \pmod r$

फिर वह मैट्रिक्स C को एलिस को भेजता है।

#### A.2.3 साझा गुप्त कुंजी की गणनाः

1. एलिस को बॉब द्वारा भेजी गई मैट्रिक्स C प्राप्त होती है, और उसके पास अपनी निजी कुंजी a होती है। वह बॉब की सार्वजनिक मैट्रिक्स पर अपनी निजी कुंजी लागू करती है:

$S = C^a \pmod r = (B^b)^a \pmod r$

2. बॉब को एलिस द्वारा भेजी गई मैट्रिक्स A प्राप्त होती है, और उसके पास अपनी निजी कुंजी b होती है। वह एलिस की सार्वजनिक मैट्रिक्स पर अपनी निजी कुंजी लागू करता है:

$S = A^b \pmod r = (B^a)^b \pmod r$

3. चूंकि मैट्रिक्स घातांक (exponentiation) साहचर्य नियम (associative law) का पालन करते हैं, इसलिए यह सुनिश्चित किया जा सकता है कि:

$S = (B^a)^b \pmod r = B^{ab} \pmod r = (B^b)^a \pmod r$

इस प्रकार, एलिस और बॉब दोनों को एक ही साझा गुप्त मैट्रिक्स प्राप्त होती है।

### A.3 सुरक्षा विचार

इस योजना की मजबूती एक गहरे गणनात्मक अवरोध पर निर्भर करती है: A, C, और B दिए जाने पर, a या b का अनुमान लगाने के लिए मैट्रिक्स क्षेत्र में विविक्त लघुगणक समस्या को हल करना आवश्यक होता है [18], जो बड़े r के लिए गणनात्मक रूप से असंभव माना जाता है [3]। यह इसके स्केलर पूर्वज (scalar progenitor) की मजबूती के समान है, लेकिन मैट्रिक्स विस्तार इसकी उपयोगिता को बढ़ाता है, जिससे आधुनिक नेटवर्क सुरक्षा के लिए महत्वपूर्ण प्रक्रियाओं जैसे सुरक्षित बहु–आयामी कुंजी समझौतों और रूपांतरणों का समर्थन होता है [12, 19]।

## B. संदेश संचरण का आलेख सैद्धांतिक निरूपण

आलेख सिद्धांत, [14] संदेश प्रसारण को मॉडल और विश्लेषण करने का एक व्यवस्थित ढंग प्रदान करता है जिसमे मुख्यतः इसे भारित कोरों (weighted edges) के साथ एक पूर्ण आलेख के जरिए निरूपित किया जाता है। इस निरूपण में, प्रत्येक शीर्ष (vertex) एनकोडेड संदेश के एक हिस्से के संगत होता है, और कोर (edges) संख्यात्मक अंतरों के आधार पर उनके बीच संबंधों को दर्शाते हैं। इस अनुभाग में वर्तमान तकनीकों में प्रयुक्त निम्नलिखित अवधारणाएँ वर्णित की गई हैं:

1. पूर्ण आलेख निरूपण
2. शीर्ष संख्या निर्धारण के लिए एन्कोडिंग तालिका
3. आपतन शीर्ष के अंतर का उपयोग करते हुए भारित कोर

### B.1 पूर्ण आलेख निरूपण

एक पूर्ण आलेख वह आलेख होता है जिसमें प्रत्येक भिन्न युग्म शीर्षों (vertices) के बीच एक किनारा (edge) होता है [14, 16] जब संदेश संचरण (message transmission) का मॉडल तैयार किया जाता है, तो निम्नलिखित परंपरा अपनाई जाती है:

• प्रत्येक शीर्ष एन्कोड किए गए संदेश में एक प्रतीक या वर्ण का प्रतिनिधित्व करता है।

• शीर्षों के बीच के किनारे इन प्रतीकों के बीच की परस्पर क्रिया या संक्रमण को दर्शाते हैं।

चूंकि एक पूर्ण आलेख यह सुनिश्चित करता है कि सभी प्रतीक एक–दूसरे को प्रभावित करते हैं, अर्थात् इसमें संपूर्ण संपर्कता (exhaustive connectivity) होती है। इससे यह सुनिश्चित होता है कि प्रत्येक प्रतीक अपने साथियों पर प्रभाव डालता है। यह संरचना विशेष रूप से कूटलेखन, त्रुटि पहचान (error detection), और नेटवर्क संप्रेषण (communication) मॉडल में उपयोगी होती है [16]।

**B. 2 शीर्ष क्रमांकन के लिए एन्कोडिंग तालिका** (Encoding Table for Vertex Numbering)

संदेश में प्रयुक्त प्रत्येक प्रतीक को नीचे दी गई एन्कोडिंग तालिका के आधार पर एक विशिष्ट संख्यात्मक मान दिया गया है:

**तालिका–1:**

| $f(V_{ij})$ | **0** | **1** | **2** | **3** | **4** | **5** |
|---|---|---|---|---|---|---|
| **1** | A | B | C | D | E | F |
| **2** | G | H | I | J | K | L |
| **3** | M | N | O | P | Q | R |
| **4** | S | T | U | V | W | X |
| **5** | Y | Z | - | ? | . | ! |

इस एन्कोडिंग के एक उदाहरण मे हम देखते हैं, कि निम्नलिखित कोड प्राप्त किए जा सकते हैं:

$$f(V_{10}) = f(A) = 10$$

$$f(V_{40}) = f(S) = 40$$

$$f(V_{43}) = f(V) = 43$$

$$f(V_{31}) = f(N) = 31$$

$$f(V_{22}) = f(I) = 22$$

$$f(V_{41}) = f(T) = 41$$

**B.3 आपतित शीर्षों के अंतर का उपयोग करते हुए भारित किनारे**

पूर्ण आलेख में किनारों को उन शीर्षों के संख्यात्मक अंतर के आधार पर भार (weight) दिया जाता है, जिनसे वे जुड़े होते हैं। उदाहरण के लिए, यदि दो शीर्ष V और N को मान f(V) और f(N) दिए गए हैं, तो उनके बीच के किनारे का भार इस प्रकार निकाला जाता है:

$$W_{VN} = |f(V) - f(N)| = |43 - 31| = 12$$

यह सुनिश्चित करता है कि:

• प्रतीकों के मानों में अधिक अंतर होने पर भार भी अधिक होगा।

• भार वितरण (weight distribution) एन्कोड किए गए संदेश में विविधताओं को दर्शाता है।

• यह संदेश की जटिलता का विश्लेषण आलेख–सिद्धांत आधारित मापदंडों द्वारा करने का एक तरीका प्रदान करता है [16]।

### C. चेबिशेव बहुपद और उनके गुण

चेबिशेव बहुपद [15] प्रस्तावित कूटलेखन योजना के लिए एक सशक्त गणितीय आधार प्रदान करते हैं। ये बहुपद अपनी लाम्बिक संरचना, अराजक गतिकी (chaotic dynamics), और सीमित क्षेत्रों (finite fields) में आवर्ती गुणों (periodic properties) का लाभ उठाते हैं।

इस अनुभाग में इन बहुपदों की परिभाषा दी गई है, इनके समाकलनों (integrals) को एक विश्लेषणात्मक विस्तार के रूप में प्रस्तुत किया गया है, और इनके गुणों यथा अराजक व्यवहार (chaotic behavior), सेमीग्रुप गुण (semigroup property) और मापांक अंकगणित (modular arithmetic) के अंतर्गत आवर्तिता (periodicity) का विवरण दिया गया है। ये सभी गुण इस कूटलेखन प्रणाली की क्रिप्टोग्राफिक मजबूती में महत्वपूर्ण योगदान देते हैं [1]।

### C.1. चेबिशेव बहुपद (Chebyshev Polynomials)

चेबिशेव बहुपद [15], जिन्हें $T_n(x)$ से निरूपित किया जाता है, लाम्बिक बहुपद (orthogonal polynomials) का अनुक्रम होता है जो पुनरावृत्तिपूर्वक रूप मे इस प्रकार परिभाषित है:

$$T_0(x) = 1$$

$$T_1(x) = x$$

$$T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x), \text{for } n \geq 2$$

### C.2 चेबिशेव अराजकीय व्यवहार

चेबिशेव बहुपद (Chebyshev polynomials) कुछ विशेष क्षेत्रों, विशेषकर अंतराल $x \in [-1,1]$, में पुनरावृत्त (iterate) करने पर अराजकीय (chaotic) व्यवहार प्रदर्शित करते हैं। अराजक गुण को समीकरण $T_n(x) = co(n\cos^{-1}(x))$ अथवा $T_2(x) = 2x^2 - 1$ द्वारा दर्शाया जाता है [17]। यह रूपांतरण प्रारंभिक स्थितियों पर अत्यधिक निर्भरता को दर्शाता है जो अराजक मानचित्रों (chaotic maps) की एक विशेषता है जिससे बिना x के सटीक ज्ञान के अनुक्रम (sequence) को पूर्वानुमानित करना असंभव हो जाता है [17]। ऐसा अराजक व्यवहार बलपूर्वक डिकोडिंग (brute-force decipherment) के विरुद्ध एन्क्रिप्शन को अधिक मजबूत बनाता है।

### C.3 माड्यूलो p के अंतर्गत चेबिशेव बहुपदों का विस्तारित सेमिग्रुप गुण

चेबिशेव बहुपदों का एक मूलभूत गुण उनका सेमिग्रुप संरचना (semigroup structure) होना है [15]।

जब किसी अभाज्य संख्या ppp के साथ माड्यूलर अंकगणित (modular arithmetic) किया जाता है, तो चेबिशेव बहुपद एक समान संरचना को बनाए रखते हैं:

$$T_m(T_n(x)) = T_n(T_m(x)) = T_{mn}(x)$$

इसका तात्पर्य यह है कि चेबिशेव बहुपदों की गुणात्मक विशेषताएँ, जैसे संयोजन पर स्थायित्व (closure under composition), माड्यूलो p के अंतर्गत भी बनी रहती हैं, जो क्रिप्टोग्राफिक एल्गोरिथ्म में इन्हें विशेष रूप से उपयोगी बनाती हैं।

$$T_m(T_n(x \bmod p)) \bmod p = T_n(T_m(x \bmod p)) \bmod p = T_{mn}(x \bmod p) \bmod p$$

### C.4. चेबिशेव अनुक्रम का आवर्ती व्यवहार

चेबिशेव अनुक्रम, मापांक अंकगणित (modular arithmetic) के अंतर्गत गणना किए जाने पर आवर्ती (periodic) व्यवहार प्रदर्शित करता है। चूँकि परिमित क्षेत्र (finite fields) में तत्वों की संख्या सीमित होती है, इसलिए चेबिशेव बहुपदों (Chebyshev polynomials) को दोहराने पर चक्रीय (cyclic) स्वरूप प्राप्त होता है। अर्थात, किसी निश्चित आवर्त t के लिए हम पाते हैं कि

$$T_n(x) = T_{n+l}(x) \bmod p$$

यह उल्लेखनीय है कि चेबिशेव बहुपद अनुक्रम का आवर्त

$\{T_n(x)\}_{n\geq 0} \bmod p (\text{odd prime}) \text{ for each } x = 0,1,2,...,p-1, p^2-1$ का एक भाजक है

उदाहरण : अनुक्रम $\{T_n(x)\}_{n\geq 0} \bmod 19$ प्रत्येक $x = 0,1,2,...,18$ का आवर्त निम्नलिखित से दिया जाता है:

$x = 0 : 0,1,0,18,0,1,0,18,0...$ (period 4),

$x = 1 : 1,1,1,1,1,1...$ (period 0),

$x = 2 : 2,1,2,7,7,2,1,2,7,7,2...$ (period 5),

$x = 3 : 3,1,3,17,4,7,0,12,15,2,16,18,16,2,15,12,0,7,4,17,3...$ (period 20),

$x = 4 : 4,1,4,12,16,2,0,17,3,7,15,18,15,7,3,17,0,2,16,12,4...$ (period 20),

$x = 0$ $x = 0$ $x = 0$ से 18 18 18 तक के आवर्त की तालिका $192-1=360$ $19\hat{}2-1=360$ $192-1=360$ के भाजक प्रकट करती है:

| X | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Period | 4 | 1 | 5 | 20 | 20 | 18 | 18 | 5 | 18 | 3 | 6 | 9 | 10 | 9 | 9 | 20 | 20 | 10 | 2 |

यहाँ सभी आवर्त $19^2 - 1 = 20 \times 18$ के भाजक हैं। यह सुगमता से सत्यापित किया जा सकता है कि किसी भी विषम अभाज्य संख्या p के आवर्त सदैव $x = 0$, $x = 1$ और $x = p-1$ के लिए क्रमशः 4, 1, और 2 हैं।

### D. कोकेरेव द्वारा चेबिशेव बहुपदों का उपयोग करके RSA योजना

लियोनार्ड कोकेरेव [17] ने एक RSA–जैसी एन्क्रिप्शन योजना का प्रस्ताव किया, जो चेबिशेव बहुपदों के अराजक गुणों का उपयोग करती है। इस विधि का मूल विचार यह है कि RSA में प्रयुक्त मापांक घातांक (modular exponentiation) को चेबिशेव बहुपदों के संयोजन गुण (composition property) से प्रतिस्थापित किया जाए। यह दृष्टिकोण बहुपदों के अराजक स्वभाव का लाभ उठाकर सुरक्षा को बढ़ाता है, जबकि RSA की गुणनखंडन–आधारित नींव को बरकरार रखता है [1]।

### D.1. कुंजी निर्माण

कुंजी निर्माण की प्रक्रिया में निम्नलिखित चरण होते हैं:

1. दो बड़ी अभाज्य संख्याएँ p और q चुनें, और फिर $N = pq$ तथा $N^* = (p^2-1)(q^2-1)$ की गणना करें।
2. एक निजी पूर्णांक d चुनें और उसका मापांक प्रतिलोम (modular inverse) e इस प्रकार ज्ञात करें कि $ed \equiv 1 \bmod N^*$, $(e, N)$ सार्वजनिक कुंजी है और d निजी कुंजी है।

### D.2. कूटन

एक संदेश $x : 1 \le x \le N,$ के लिए कूटलिखित पाठ्यांश (ciphertext) का परिकलन निम्नलिखित प्रकार से होगाः

$$C = T_e(x) \bmod N$$

यहाँ $T_e(x) \bmod N$ चेबिशेव बहुपद (Chebyshev polynomial) है, जिसकी डिग्री e है, और जिसे x पर मापांक N (modulo N) के अंतर्गत मूल्यांकित किया गया है [15]।

### D.3. विकूटन

मूल संदेश x को पुनः प्राप्त करने के लिए निम्नलिखित गणना करें:

$$x = T_d(C) (\bmod N)$$

### D.4. डिक्रिप्शन योजना का सत्यापन

यहाँ कुछ महत्वपूर्ण अवलोकन हैं:

1. विकूटन (decryption) सफल होता है क्योंकि $T_e(T_d(x)) = T_{e.d}(x),$ और चूंकि $e.d \equiv 1 (\bmod N^*),$ अतः $T_{e.d}(x) \equiv T_1(x) \equiv x (\bmod N)$ [17].

2. इसी प्रकार $T_d(T_e(x)) \equiv x (\text{mod} N)$ । चाइनीज शेषफल प्रमेय (Chinese Remainder Theorem) यह सुनिश्चित करता है कि यह अलग अलग अविभाज्य संख्याओं p और q मे मान्य राहत है।

इन बिन्दुओं को निम्नलिखित तरीके से सविस्तार समझाया जा सकता है:

$$ed \equiv 1 \bmod N^* \Rightarrow ed = 1 + kN^* = 1 + k(p^2 - 1)(q^2 - 1),$$

$$T_{ed}(x) \bmod p \equiv T_{1+kN^*}(x) \bmod p \equiv T_1(x) \bmod p \equiv x \bmod p \quad \because p \mid N^*$$

समान तर्क का उपयोग करते हुए,

$$T_{ed}(x) \bmod q \equiv T_{1+kN^*}(x) \bmod q \equiv T_1(x) \bmod q \equiv x \bmod q \quad \because q \mid N^*$$

चूंकि p और q अलग अलग संख्याएं हैं, अतः चाइनीज शेषफल प्रमेय (Chinese Remainder theorem) के प्रयोग से

$$T_{ed}(x) \bmod N \equiv T_{1+kN^*}(x) \bmod N \equiv T_1(x) \bmod N \equiv x \bmod N$$

### D.5. सुरक्षा विचार

- यह स्पष्ट है कि चेबिशेव–आधारित RSA की सुरक्षा इस पर निर्भर करती है कि बिना निजी कुंजी के चेबिशेव बहुपदों का व्युत्क्रम (inverse) निकालना कितना कठिन है। इस समस्या का कोई प्रभावी समाधान उपलब्ध नहीं है [15]। इसके अतिरिक्त, चेबिशेव बहुपदों का अराजक व्यवहार (chaotic behaviour) इसे अप्रत्याशितता की एक अतिरिक्त परत प्रदान करता है [17]। इस योजना की सुरक्षा पारंपरिक RSA की तरह गुणनखंडन समस्या (factoring problem) पर भी निर्भर करती है। चूंकि मापांक N को दो बड़ी अभाज्य संख्याओं p और q के गुणनफल के रूप में चुना जाता है, इसलिए एनक्रिप्शन

को तोड़ने के लिए N को $N^* = (p^2 - 1)(q^2 - 1)$ फैक्टर करना आवश्यक होगा जो कि बड़े अंकों के लिए व्यावहारिक रूप से असंभव है [4]।

**प्रस्तावित योजना का एक उदाहरण द्वारा चित्रण**

- जैसा कि पिछले अनुभाग में वर्णित किया गया है, प्रस्तावित कूटलेखन योजना में संदेश को एक पूर्ण आलेख के बाहरी हैमिल्टोनियन पथ (outer Hamiltonian path) के शीर्षों (vertices) पर एन्कोड किया जाता है। किनारों (edges) का भारनिर्धारण संबंधित आपतन शीर्षों (incident vertices) के एन्कोड किए गए मानों के अंतर के आधार पर निर्धारित किया जाता है। इसके बाद, पूर्ण आलेख के भारित आसन्नता आव्यूह (weighted adjacency matrices) का निर्माण किया जाता है और इसे एक साझा कुंजी आव्यूह (shared key matrix) से गुणा किया जाता है, जिसे आव्यूह – आधारित डिफ्फी–हेलमैन कुंजी विनिमय योजना के माध्यम से सुरक्षित रूप से साझा किया गया होता है।

  प्राप्त मैट्रिक्स को फिर कोकेरेव द्वारा प्रस्तावित चेबिशेव–RSA योजना का उपयोग करके एन्क्रिप्ट किया जाता है। डिक्रिप्शन के लिए, एन्क्रिप्टेड आव्यूह को पहले चेबिशेव–RSA योजना का उपयोग करके डिक्रिप्ट किया जाता है। उसके बाद, परिणाम को साझा कुंजी आव्यूह के व्युत्क्रम (inverse) से गुणा किया जाता है। अंत में, भारित आसन्नता आव्यूह और एन्कोडिंग तालिका का उपयोग करके संदेश को चरण–दर–चरण पुनर्प्राप्त किया जाता है। नीचे एक विस्तृत चरण–दर–चरण प्रक्रिया को एक उदाहरण सहित प्रस्तुत किया गया है।

  एन्क्रिप्शन प्रक्रिया शुरू करने से पहले, एलिस और बॉब संदेश की लंबाई के आधार पर आव्यूह – आधारित डिफी–हेलमैन कुंजी विनिमय विधि का उपयोग करके एक साझा कुंजी आव्यूह स्थापित करते हैं।

  मान लीजिए एलिस बॉब को पाँच अक्षरों का संदेश भेजना चाहती है। दोनों एक 5×5 आधार आव्यूह B और एक अभाज्य संख्या r पर सहमत होते हैं:

$$B = \begin{pmatrix} 1 & 2 & 4 & 5 & 6 \\ 3 & 4 & 9 & 2 & 7 \\ 5 & 6 & 2 & 1 & 3 \\ 4 & 5 & 7 & 3 & 5 \\ 7 & 3 & 4 & 5 & 8 \end{pmatrix} \text{ एवं } r = 11$$

**कुंजी विनिमय**

- निजी कुंजी चयन

  एलिस एक निजी पूर्णांक a=3 चुनती है, जो गुप्त रहता है।

  बॉब एक निजी पूर्णांक b=4 चुनता है, जो गुप्त रहता है।

- सार्वजनिक कुंजी का परिकलन

  एलिस सार्वजनिक कुंजी का परिकलन करती है:

$$A \equiv B^{a} \bmod r \equiv B^{3} \bmod 11$$

$$A \equiv \begin{pmatrix} 1732 & 1625 & 2053 & 1387 & 2470 \\ 2243 & 2092 & 2714 & 1821 & 3252 \\ 1700 & 1544 & 1793 & 1213 & 2200 \\ 2210 & 2058 & 2573 & 1709 & 3089 \\ 2607 & 2392 & 2955 & 2008 & 3567 \end{pmatrix} \bmod 11$$

$$A = \begin{pmatrix} 5 & 8 & 7 & 1 & 6 \\ 10 & 2 & 8 & 6 & 7 \\ 6 & 4 & 0 & 3 & 0 \\ 10 & 1 & 10 & 4 & 9 \\ 7 & 5 & 7 & 6 & 3 \end{pmatrix}$$

और A, बॉब को प्रेषित कर देती है।

- बॉब सार्वजनिक आव्यूह का परिकलन करता है:

$$C \equiv B^{b} \bmod r \equiv B^{4} \bmod 11$$

$$C \equiv \begin{pmatrix} 37910 & 36627 & 45248 & 30474 & 54621 \\ 52137 & 47999 & 58983 & 39836 & 71365 \\ 35549 & 32999 & 41573 & 28020 & 50052 \\ 49708 & 45902 & 56827 & 38311 & 68642 \\ 57559 & 53253 & 66190 & 44633 & 79827 \end{pmatrix} \bmod 11$$

$$C = \begin{pmatrix} 0 & 8 & 5 & 4 & 6 \\ 8 & 6 & 1 & 5 & 8 \\ 8 & 10 & 4 & 3 & 2 \\ 10 & 10 & 1 & 9 & 2 \\ 7 & 2 & 3 & 6 & 0 \end{pmatrix}$$

और C एलिस को प्रेषित कर देता है।

**साझा कुंजी का परिकलन**

एलिस परिकलित करती है:

$$S \equiv C^{a} \equiv B^{ba} \bmod r$$

$$S \equiv \begin{pmatrix} 3444 & 4322 & 1653 & 3279 & 2670 \\ 4376 & 4938 & 1784 & 3835 & 2854 \\ 4508 & 4800 & 1837 & 3888 & 2936 \\ 5564 & 5970 & 2186 & 4859 & 3634 \\ 3246 & 3460 & 1207 & 2720 & 2176 \end{pmatrix} \bmod 11$$

$$S = \begin{pmatrix} 1 & 10 & 3 & 1 & 8 \\ 9 & 10 & 2 & 7 & 5 \\ 9 & 4 & 0 & 5 & 10 \\ 9 & 8 & 8 & 8 & 4 \\ 1 & 6 & 8 & 3 & 9 \end{pmatrix} \text{अ}$$

बॉब परिकलन करता है:

$$S \equiv A^b \equiv B^{ab} \bmod r$$

$$S \equiv \begin{pmatrix} 95635 & 70080 & 96143 & 60853 & 74511 \\ 115960 & 84567 & 116074 & 72915 & 90414 \\ 57154 & 39450 & 56034 & 35711 & 43933 \\ 111978 & 83432 & 113055 & 70540 & 87850 \\ 76242 & 55567 & 75732 & 48920 & 58672 \end{pmatrix} \bmod 11$$

$$S = \begin{pmatrix} 1 & 10 & 3 & 1 & 8 \\ 9 & 10 & 2 & 7 & 5 \\ 9 & 4 & 0 & 5 & 10 \\ 9 & 8 & 8 & 8 & 4 \\ 1 & 6 & 8 & 3 & 9 \end{pmatrix}$$

चूंकि आव्यूह घातांक, गुणन साहचर्य नियम का पालन करता है:

$$(B^a)^b = (B^b)^a \equiv B^{ab} \bmod r$$

**एन्क्रिप्शन योजना:**

- एलिस एन्क्रिप्शन प्रक्रिया की शुरुआत मूल संदेश "SVNIT" से करती है। चूंकि यह संदेश पाँच अक्षरों का है, वह एक पूर्ण आलेख K5 बनाती है और प्रत्येक अक्षर को आलेख के शीर्षों (vertices) पर एक विशिष्ट सांकेतिक संख्यात्मक मान (encoded numerical value) सौंपती है। इसके बाद, वह किनारों (edges) के भारों (weights) की गणना उन संबंधित शीर्षों के सांकेतिक मानों के परस्पर अनुपात (absolute difference) के रूप में करती है।

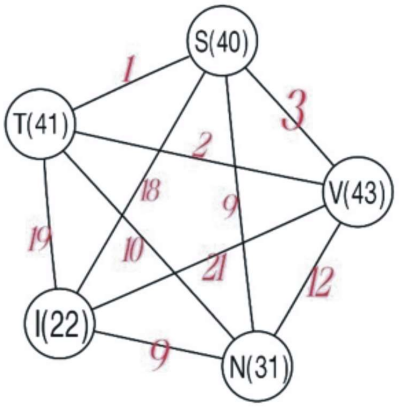
$W_{SV} = |f(V) - f(S)||43 - 40| = 3$

$W_{VN} = |f(N) - f(V)||31 - 43| = 12$

$W_{NI} = |f(I) - f(N)||22 - 31| = 9$

$W_{IT} = |f(T) - f(I)||41 - 22| = 19$

$W_{TS} = |f(S) - f(T)||40 - 41| = 1$ और इसी प्रकार




- एलिस पूर्ण आलेख K5 से प्राप्त किए गए किनारों के भारों (edge weights) के आधार पर भारित आसन्नता आव्यूह (weighted adjacency matrix) का निर्माण करती है।

$$M = \begin{array}{c} \\ S \\ V \\ N \\ I \\ T \end{array} \begin{array}{c} \begin{array}{ccccc} S & V & N & I & T \end{array} \\ \begin{pmatrix} 0 & 3 & 9 & 18 & 1 \\ 3 & 0 & 12 & 21 & 9 \\ 9 & 12 & 0 & 9 & 10 \\ 18 & 21 & 9 & 0 & 19 \\ 1 & 2 & 10 & 19 & 0 \end{pmatrix} \end{array}$$

- ऐलिस प्रारंभिक अक्षर के कूटबद्ध मान (encoded value) को विकर्ण की सबसे ऊपरी–बाएँ स्थिति में लिखती है।

$$M_1 = \begin{array}{c} \\ S \\ V \\ N \\ I \\ T \end{array} \begin{array}{c} \begin{array}{ccccc} S & V & N & I & T \end{array} \\ \begin{pmatrix} \mathit{40} & \mathit{3} & 9 & 18 & 1 \\ 3 & 0 & \mathit{12} & 21 & 9 \\ 9 & 12 & 0 & \mathit{9} & 10 \\ 18 & 21 & 9 & 0 & \mathit{19} \\ 1 & 2 & 10 & 19 & 0 \end{pmatrix} \end{array}$$

- इसे साझा आव्यूह S से गुणा करके एलिस परिकलित करती है

$$E = M_1.S = \begin{pmatrix} 311 & 616 & 278 & 253 & 506 \\ 302 & 258 & 193 & 237 & 246 \\ 208 & 342 & 203 & 195 & 258 \\ 307 & 540 & 248 & 267 & 510 \\ 280 & 222 & 159 & 217 & 194 \end{pmatrix}$$

- इसके बाद, इस आव्यूह को चेबिशेव–RSA(Chebyshev-RSA scheme) योजना का उपयोग करके एन्क्रिप्ट किया जाता है।

  बॉब दो अभाज्य संख्याएँ p=23 तथा q=29 चुनता है, और निम्नलिखित गणनाएँ करता है:

  $N = pq = 23 \times 29 = 667$

  फिर वह परिकलन करता है:

  $N^* = (p^2 - 1)(q^2 - 1) = 443520$

  बॉब $e = 13$ का चयन करता है और d का परिकलन इस प्रकार से करता है:

  $ed \equiv 1 \bmod N^*$

  d के लिए हल करने पर, वह प्राप्त करता है:

  $d = 34117$

  फिर बॉब e और N को सार्वजनिक कर देता है।

- अब एलिस परिकलन करती है:

  $F \equiv T_{13}(E) \bmod 667$

$$F = \begin{pmatrix} 472 & 503 & 490 & 414 & 506 \\ 293 & 394 & 497 & 488 & 478 \\ 24 & 6 & 464 & 356 & 394 \\ 606 & 540 & 480 & 400 & 548 \\ 410 & 613 & 246 & 565 & 542 \end{pmatrix}$$

  एलिस अंतिम एन्क्रिप्टेड मैट्रिक्स के रूप में F को बॉब को भेजती है।

**विकूटन योजना:**

- बॉब अपनी निजी कुंजी का उपयोग करके प्राप्त करता है – $E \equiv T_{34117}(F) \bmod 667$

$$E = \begin{pmatrix} 311 & 616 & 278 & 253 & 506 \\ 302 & 258 & 193 & 237 & 246 \\ 208 & 342 & 203 & 195 & 258 \\ 307 & 540 & 248 & 267 & 510 \\ 280 & 222 & 159 & 217 & 194 \end{pmatrix}$$

विकूटन प्रक्रिया का सत्यापन निम्नलिखित प्रकार से किया गया है:

$$T_d(T_e(E) \bmod pq) \bmod pq \equiv T_{de}(E) \bmod pq$$

$$T_{de}(E) \bmod pq \equiv T_{(1+1.N^*)}(E) \bmod pq \equiv T_1(E) = E$$

- अब, बॉब साझा कुंजी आव्यूह $S^{-1}$ के व्युत्क्रम (inverse) से E को गुणा करके $M_1$ को पुनः प्राप्त करता है।

- $$M1 = E.S^{-1} = \begin{pmatrix} 311 & 616 & 278 & 253 & 506 \\ 302 & 258 & 193 & 237 & 246 \\ 208 & 342 & 203 & 195 & 258 \\ 307 & 540 & 248 & 267 & 510 \\ 280 & 222 & 159 & 217 & 194 \end{pmatrix} . \frac{1}{9504} \begin{pmatrix} 2880 & -4320 & 1728 & 3744 & -3744 \\ 1110 & 315 & -522 & 156 & -651 \\ 1212 & -2610 & 252 & 2328 & -942 \\ -5392 & 7032 & -1968 & -5056 & 5320 \\ -340 & 246 & 588 & -904 & 970 \end{pmatrix}$$

- $$M_1 = \begin{array}{c} \\ S \\ V \\ N \\ I \\ T \end{array} \begin{array}{c} \begin{array}{ccccc} S & V & N & I & T \end{array} \\ \begin{pmatrix} \textit{40} & \textit{3} & 9 & 18 & 1 \\ 3 & 0 & \textit{12} & 21 & 9 \\ 9 & 12 & 0 & \textit{9} & 10 \\ 18 & 21 & 9 & 0 & \textit{19} \\ 1 & 2 & 10 & 19 & 0 \end{pmatrix} \end{array}$$

बॉब भारित आसन्नता आव्यूह (weighted adjacency matrix) के विकर्ण (diagonal) की प्रथम प्रविष्टि (entry) के साथ सुपर–विकर्ण (super-diagonal) प्रविष्टियों का उपयोग करता है। एक सरल गणना प्रक्रिया के माध्यम से, वह पूर्ण आलेख (complete graph) का पुनर्निर्माण करता है। इस पुनर्निर्मित आलेख और एन्कोडेड तालिका (encoded table) का उपयोग करके, बॉब मूल संदेश SVNIT को सफलतापूर्वक डिकोड करता है।

## निष्कर्ष

प्रस्तावित एन्क्रिप्शन तकनीक आलेख सिद्धांत, कुंजी विनिमय तंत्र, और चेबिशेव बहुपदों के साथ RSA एन्क्रिप्शन का सफलतापूर्वक एकीकरण करती है, इस प्रकार एक बहु–स्तरीय सुरक्षा दृष्टिकोण प्रदान करती है। पूर्ण आलेख की भारित आसन्नता आव्यूह का उपयोग करके, यह विधि संदेश को कुशलतापूर्वक एन्कोड करते हुए मजबूत गूढ़ालेखी सुरक्षा भी सुनिश्चित करती है [14]। डिफ्फी–हेलमैन आव्यूह – आधारित कुंजी विनिमय साझा गुप्त व्युत्पत्ति (shared secret derivation) के माध्यम से गोपनीयता को बढ़ाता है, जबकि चेबिशेव बहुपदों का अराजक व्यवहार एन्क्रिप्शन को हमलों के प्रति अधिक प्रतिरोधी बनाता है।

पारंपरिक गूढ़ालेखी तकनीकों की तुलना में, यह दृष्टिकोण डिस्क्रीट लॉगरिद्म समस्या और पूर्णांक गुणनखंडन समस्या दोनों का लाभ एक साथ उठाता है, जिससे संभावित हमलावरों के लिए जटिलता काफी बढ़ जाती है। प्रस्तावित योजना न केवल मजबूत सुरक्षा और गणनात्मक दक्षता सुनिश्चित करती है, बल्कि यह सुरक्षित संचार और डेटा सुरक्षा में वास्तविक अनुप्रयोगों के लिए भी उपयुक्त है।

### भविष्य के अनुसंधान का दायरा

इस प्रणाली की गणनात्मक दक्षता को अनुकूलित करने, क्वांटम हमलों के प्रति प्रतिरोध का अन्वेषण करने, और इसे ब्लॉकचेन तथा सुरक्षित क्लाउड कंप्यूटिंग जैसे क्षेत्रों में विस्तारित करने पर केंद्रित हो सकता है। यह अध्ययन आलेख – सिद्धांत आधारित कूटलेखन को संख्या–सैद्धांतिक (number-theoretic) सुरक्षा सिद्धांतों के साथ संयोजित करने की संभावनाओं को दर्शाते हुए आधुनिक क्रिप्टोग्राफिक प्रणालियों की प्रगति में एक महत्वपूर्ण योगदान देता है।

## संदर्भ


1. Katz, J., & Lindell, Y. (2021). Introduction to Modern Cryptography (3rd ed.). Chapman & Hall/CRC. https://doi.org/10.1201/9781351133036 (Utility in cryptography)
2. Diffie, W., & Hellman, M. (1976). New Directions in Cryptography. IEEE Transactions on Information Theory, 22(6), 644-654. https://doi.org/10.1109/TIT.1976.1055638
3. Shor, P. W. (1997). Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM Journal on Computing, 26(5), 1484-1509. https://doi.org/10.1137/S0097539795293172
4. Rivest, R. L., Shamir, A., & Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, 21(2), 120-126. https://doi.org/10.1145/359340.359342
5. Boneh, D., & Shoup, V. (2020). A Graduate Course in Applied Cryptography. https://toc.cryptobook.us/
6. ElGamal, T. (1985). A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. IEEE Transactions on Information Theory, 31(4), 469-472. https://doi.org/10.1109/TIT.1985.1057074
7. Schnorr, C. P. (1991). Efficient Identification and Signatures for Smart Cards. Advances in Cryptology - CRYPTO '89, 239-252. https://doi.org/10.1007/0-387-34805-0_22
8. National Institute of Standards and Technology (NIST). (2020). Digital Signature Standard (DSS). Federal Information Processing Standards Publication 186-4. https://doi.org/10.6028/NIST.FIPS.186-4
9. Buchmann, J., Dahmen, E., & Hülsing, A. (2019). Post-Quantum Signatures: A Survey. Journal of Mathematical Cryptology, 13(2), 73-99. https://doi.org/10.1515/jmc-2018-0010
10. Toral, R. (2005). On the Use of Chebyshev Polynomials in Discrete-Time Cryptography. Chaos, Solitons & Fractals, 24(4), 1117-1126. https://doi.org/10.1016/j.chaos.2004.09.066
11. Alvarez, G., & Li, S. (2006). Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems. International Journal of Bifurcation and Chaos, 16(8), 2129-2151. https://doi.org/10.1142/S0218127406015970
12. Bernstein, D. J., & Lange, T. (2022). Post-Quantum Cryptography: State of the Art. Journal of Cryptology, 35(1), 1-25. https://doi.org/10.1007/s00145-021-09412-3
13. NIST. (2023). Post-Quantum Cryptography Standardization: Round 4 Report. https://csrc.nist.gov/projects/post-quantum-cryptography
14. Diestel, R. (2017). Graph Theory. Springer. https://doi.org/10.1007/978-3-662-53622-3
15. Dubey, A., Kumar, S., & Sharma, P. (2020). Introduction to Chebyshev Polynomials and Their Applications in Cryptography. Springer. (Chebyshev foundation)

16. Gross, J. L., & Yellen, J. (2003). Graph Theory and Its Applications (2nd ed.). Chapman & Hall/CRC. https://doi.org/10.1201/9780203490204

17. Kocarev, L. (2001). Chaos-Based Cryptography: A Brief Overview. IEEE Circuits and Systems Magazine, 1(3), 6-21. https://doi.org/10.1109/7384.963463 (Chaos properties)

18. Odlyzko, A. M. (2000). Discrete Logarithms: The Past and Future. Designs, Codes, and Cryptography, 19(2), 129-145.

19. Chen, L., Moody, D., & Regenscheid, A. (2022). Lightweight Cryptography: NIST Standards and Applications. NISTIR 8346. https://doi.org/10.6028/NIST.IR.8346

20. Mason, J. C., & Handscomb, D. C. (2003). Chebyshev Polynomials. Chapman & Hall/CRC. https://doi.org/10.1201/9781420036114 (New: Chebyshev integrals and properties)