

RESUME



1. **Name** : Dr. P. L. Sharma
2. **Father's Name** : Shri R. D. Sharma
3. **Permanent Address** : House No. 51, Roura Sector -2,
Bilaspur (HP) Pin-174001
4. **E-mail Address** : plsharma1964@gmail.com , pl.sharma@hpuniv.ac.in
5. **Own Website Address** : www.plsharma.in
6. **Place of Birth** : Bilaspur (Himachal Pradesh), India
7. **Date of Birth** : 09-10-1964 (Ninth October One Thousand Nine Hundred
and Sixty Four)
8. **Present Designation** : Professor
9. **Department** : Mathematics and Statistics
10. **Institution** : Himachal Pradesh University, Shimla-5
11. **Contact No** : 94180-03066 (M), 0177-2833769(O)
12. **Areas of Interest** : Finite Fields, Cryptography, Rhotrices, Bent Functions.
13. **Qualification** : M. Phil., Ph. D. [Mathematics], MCA.

REMARKS: All the blocks of higher education i.e. Graduation, Post Graduation, M. Phil and Ph.D. in Mathematics are passed concurrently with my Govt. regular job responsibilities and after getting the degree of Ph.D. I also did CIC and 3 years Master Degree of “**Master in Computer Application**” (MCA) from IGNOU along with same conditions of my Govt. regular job responsibilities.

Qualified Departmental Examination in Financial Administrations conducted by Himachal Pradesh Institute of Public Administration, Fairlawn, Shimla.

DETAILS OF ACADEMIC ACTIVITIES

(February 2010 Onwards)

[1] LECTURES DELIVERED:

Sr. No.	Date	No. of Lectures	Topic	Institution
1.	30-11-2010	2	Basics of Mathematics	SCERT, Solan, H.P.
2.	22-12-2010	2	Applications of Mathematics in other sciences	SCERT, Solan, H.P.
3.	3-01-2011	2	Groups & Rings	ASC-BPS Mahila Vishwavidyalaya, Khanpur, [Sonipat] Haryana.
4.	4-01-2011	2	Modules & Vector Spaces	ASC-BPS Mahila Vishwavidyalaya, Khanpur, [Sonipat] Haryana.
5.	5-01-2011	2	Semirings & Smarandache Semirings	ASC-BPS Mahila Vishwavidyalaya, Khanpur, [Sonipat] Haryana.
6.	6-01-2011	2	(i) How a teacher should be? And (ii) How teaching can be effective?	ASC-BPS Mahila Vishwavidyalaya, Khanpur, [Sonipat] Haryana.
7.	28-04-2011	1	Qualities of an ideal teacher	Academic Staff College, H.P. University, Shimla.
8.	3-05-2011	2	Fundamentals of Mathematics	SCERT, Solan, H.P.
9.	23-06-2011	2	(i) Challenges and Prospects of Higher Education And (ii) How a teacher should be?	ASC-BPS Mahila Vishwavidyalaya, Khanpur, [Sonipat] Haryana.
10.	24-06-2011	2	(i) Impact of ICT on Society And (ii) How to create your own website?	ASC-BPS Mahila Vishwavidyalaya, Khanpur, [Sonipat].
11.	25-06-2011	2	(i) Challenges and Prospects of Higher Education And (ii) How a teacher should be?	ASC-BPS Mahila Vishwavidyalaya, Khanpur, [Sonipat] Haryana.

12.	29-06-2011	2	(i)Co-scholastic activities and their importance in Mathematics and (ii)Innovations and Creativity in Teaching of Mathematics	JNV Theog, Distt. Shimla for TGT(Maths.) of Chandigarh Region.
13.	1-07-2011	2	(i)Mathematics in day to day life and (ii)General Mathematical Techniques	JNV Theog, Distt. Shimla for TGT(Maths.) of Chandigarh Region.
14.	19-07-2011	1	Use of Lagrange Method for optimizations	Academic Staff College, H.P. University, Shimla.
15.	23-07-2011	1	Use of Kuhn-Tucker Method for optimizations	Academic Staff College, H.P. University, Shimla.
16.	30-05-2012	2	(i) How the teaching of a teacher can be effective (ii) Human Software and Computer Software	ASC-BPS Mahila Vishwavidyalaya, Khanpur, [Sonipat] Haryana.
17.	30-05-2012	1	Power of Human Mind	ASC-BPS Mahila Vishwavidyalaya, Khanpur, [Sonipat] Haryana.
18.	22-06-2012	2	(i) Symmetric Key Cryptography (ii) Public Key Cryptography	Rayat Bahara Institute of Engineering and Technology, Hoshiarpur (Punjab).
19.	20-07-2012 and 30-07-2012	2	(i) Quadratic Sieve (ii)Cryptography – RSA	Academic Staff College, H.P. University, Shimla.
20.	28-06-2013 and 3-07-2013	2	(i) Basics of Cryptography (ii)Discrete Logarithmic Problem	Academic Staff College, H.P. University, Shimla.
21.	12-05-14	1	“How a Teacher should be?”	ASC BPS Vishwavidyalaya, Sonapat
22.	13-05-14	1	Power of Mind and Teacher	ASC Kurukshetra University, Kurukshetra
23.	28-11-14	1	Power of Mind: Mathematics and Mathematicians	SCERT, Solan, (H. P.)
24.	1-12-15	2	1. Basics of cryptography 2. Some applications of Mathematics in Cryptography	Department of Mathematics, NIT Jalandhar

25.	16-12-15	2	1. Power of mind and Mathematician 2. Some applications of Mathematics in day to day life.	SCERT Solan, Himachal Pradesh
26.	12-06-16	2	1. Application of derivatives 2. How the teaching can be Effective?	Lecturer of Mathematics /Physics, Chemistry, Bio of DAV Schools of HP at Bilaspur
27.	14-06-16	1	Importance of Mathematics	Students of Manav Jyoti Anathalaya Ashram, Dehar, Distt. Mandi, HP
28.	14-06-16	1	How the Mathematics can be made more interesting?	Govt. Sr. Sec. School Dehar, Distt Mandi, HP
29.	10-09-16	1	How to teach Mathematics at 10+1 and 10+2 Levels	Lecturer of Mathematics of DAV Schools of HP at New Shimla
30.	23-09-16	2	1. How the teachers can motivate the students for Mathematics. 2. Role of Mathematics Teacher.	SCERT Solan, Himachal Pradesh
31.	30-08-2017	1	Applications of Higher Mathematics in Day to Day life.	Bahra University , Solan
32.	16-01-2018	1	Teaching of Mathematics at School Level.	Mathematics teachers of SVM Schools of Himachal upto 10+2 at SVM School Vikas Nagar Shimla.
33.	07-03-2018	1	Use of Mathematics in Security of Passwords.	Department of Mathematics, BPS University Khanpur (Sonipat)

[2] PAPERS PRESENTED /DELIVERED INVITED TALK/CHAired TECHNICAL SESSION IN CONFERENCES /SEMINARS :

Sr. No.	Date	Title of Paper	Title of Conference	Organising Institute
1.	20-12-2010	An application of Lagrange Multiplier and Karush Kuhn Tucker(KKT) methods	55 th Congress of Indian Society of Theoretical and applied Mechanics [An International Meet]	Department of Mathematics, NIT Hamirpur, Himachal Pradesh.

2.	5-03-2011	Problems in Higher Education	National Seminar on Education	Management & B.Ed institute, Ghanatti, Distt. Shimla, H.P.
3.	27-03-2011	Power Means with Lagrange Multiplier	National Seminar on Mathematics	Department of Mathematics, H.P University, Shimla
4.	21-10-2011 (Invited Talk)	Formulation of Some Standard Inequalities as Optimization Problems	National Conference on Role of Mathematical and Physical Sciences in Engg. and Technology	Karanprayag [Uttarakhand].
5.	22-10-2011	(Chaired Technical session)	National Conference on Role of Mathematical and Physical Sciences in Engineering and Technology	Karanprayag [Uttarakhand].
6.	06-12-2011	Constrained Multivariables Optimization and Inequalities Involving Moments	International Conference on Advances in Modeling, Optimization and Computing (AMOC-2011)	Department of Mathematics, IIT Roorkee.
7.	18-12-2011	Some Applications of Lagrangean & Karush-Kuhn-Tucker methods and Inequalities between them	1 st International Conference on Mathematical Sciences and Applications	India International Centre, New Delhi.
8.	04-02-2012	Optimization Problems in Mathematical Statistics	National Conference on Mathematics	D.A.V. Jalandhar (Punjab).
9.	23-25 October, 2013 (Invited Talk)	Rhotrices, Finite Fields with Applications in Cryptography	National Conference on Recent Trends in Algebra and Analysis (Sponsored by DST, PU Chandigarh)	A.S. College for Women, Khanna, (Punjab)
10.	23-25 October, 2013	(Chaired Technical session)	National Conference on Recent Trends in Algebra and Analysis (Sponsored by DST, PU Chandigarh)	A.S. College for Women, Khanna, (Punjab)

11.	14-17 December,2014		Indocrypt-2014	Cryptology Research society of India (CRSI) and DRDO- at Delhi
12.	13-17 July, 2015	Contributed Talk On Identification of Irreducible Polynomials over Finite Fields	International Conference on Finite Fields and Their Applications (Fq12)	New York, USA
13.	6-9 December,2015		Indocrypt-2015	Cryptology Research society of India (CRSI) IISc Bangalore
14.	27-1-2016 to 7-02-2016	Visiting Professor	Cryptology and Security Research Unit(CSRU)	ISI Kolkata
15.	16-18 December,2016		International Conference on Security, Privacy and Applied Cryptographic Engineering (SPACE-2016)	C. R. RAO Advanced Institute of Maths, Statistics &Computer Sci. (AIMSCS), Hyderabad
16.	19 - 21 January, 2017		International Conference on Mathematics and Computing (ICMC-2017),	Haldia Institute of Technology, West Bengal
17.	28-29 th March, 2017 (Invited Talk)	The role of cryptography in information and communication technology	National Conference on Recent Trends in Numerical Analysis and computational Techniques	DAV IET Jalandhar, Punjab
18.	April 07-08, 2017 (Invited Talk)	Cryptography and RSA Cryptosystem in everyday Life	National Conference on Advances in Basic & Applied Sciences	Career Point University, Hamirpur, India
19.	May 25-26, 2017 (Invited Talk)	RSA Cryptosystem in Cryptography	National Conference on Changing Trends, Future Challenges and Innovations in Science & Technology	APG Shimla University

[3] BOOKS :

Sr. No.	Title of Book	Publisher	ISBN	Year of First Edition
1.	IIT-JEE Mathematics	Satya Prakashan Publication ,New Delhi	81-7684-402-0	March, 2006
2.	Mathematics for AIEEE	Satya Prakashan Publication ,New Delhi	81-7684-537-X	Nov., 2008
3.	BCA-III Mathematics-III	Director, ICDEOL, H.P.University, Shimla-5		Oct., 2011
4.	UGC—CSIR-NET Mathematics	Satya Prakashan Publication ,New Delhi	81-7684-696-1	Jan., 2012

[4] RESEARCH PUBLICATIONS :

Sr.No.	Research Paper	ISSN
1.	Sharma, P.L. and Sharma, R., <i>A note on inequalities between the moments</i> , International Journal of Theoretical & Applied Sciences, 2 (2), P. 30-33, (2010).	0975-1718
2.	Sharma, P.L. and Sharma, R ., <i>some optimization problems related with inequalities between the moments</i> , Bulletin of Pure and Applied Sciences Volume 30 E (Math & Stat.) Issue (No.1) P. 135-144,(2011).	0970-6577
3.	Sharma, P.L. and Kanwar, R.K., <i>A note on relationship between invertible matrices and associated invertible matrices</i> , Bulletin of Pure and Applied Sciences Volume 30 E (Math & Stat.) Issue (No.2) P. 333-339, (2011).	0970-6577
4.	Sharma, P.L. and Sharma, R ., <i>Some optimization problems involving moments of discrete random variables</i> , International Journal of Theoretical & Applied Sciences, 3 (2), P. 88-90,(2011).	0975-1718
5.	Sharma, P.L. and Sharma, R., <i>On optimization problems and inequalities involving three moments</i> , International Journal of Mathematical Sciences and Applications Vol. 2, No 1, P. 245-249, Jan.(2012).	2230-9888
6.	Sharma, P.L., Sharma, R. and Thakur, A., <i>A note on inequalities involving moments of a discrete random variable</i> , International J. of Math. Sci. & Engg. Appls. (IJMSEA),Vol. 6 No. II, P. 133-143, (March, 2012).	0973-9424

7.	Sharma, P.L. and Kanwar, R.K., <i>On inner product space and bilinear forms over rhotrices</i> , Bulletin of Pure and Applied Sciences Volume 31 E (Math & Stat.) Issue (No.1) P. 109-118, (2012).	0970-6577
8.	Sharma, P.L. and Kanwar, R.K., <i>Adjoint of a rhotrix and its basic properties</i> , International Journal of Mathematical Sciences, Vol. .11, No.3-4, P.337-343, (2012).	0972-754X
9.	Sharma, P.L. and Kanwar, R.K., <i>The Cayley-Hamilton theorem for rhotrices</i> , International Journal Mathematics and Analysis, Vol.4,No.1, P.171-178, (2012).	0973-3604
10.	Sharma, P.L. and Kanwar, R.K., <i>An overview of the Cayley-Hamilton Theorem</i> , American. J. of Mathematics and Sciences, Vol. 1, No. 2,P. 249-256,(July 2012).	2250-3102
11.	Sharma, P.L. and Kanwar, R.K., <i>A note on the arithmetic function $(\sigma\phi)(n)$</i> , International J. of Math. Sci. & Engg. Appls. (IJMSEA),Vol. 6 No. V, P.145-155 , (September, 2012).	0973-9424
12.	Sharma, P.L. and Rehan, M., <i>On Security of Hill Cipher using Finite Fields</i> , International Journal of Computer Applications, Vol. 71, No.4, P. 30-33, (May 2013).	0975- 8887
13.	Sharma, P.L. and Kanwar, R.K., <i>On Involutory and Pascal rhotrices</i> , International J. of Math. Sci. & Engg. Appls. (IJMSEA),Vol. 7 No. IV, P.133-146 , (July, 2013).	0973-9424
14.	Sharma, P. L. and Kumar, S., <i>On Construction of MDS Rhotrices from Companion Rhotrices over Finite Field</i> , International Journal of Mathematical Sciences, Vol.12, No. 3-4, P. 271-286, (July-Dec., 2013).	0972-754X
15.	Sharma, P. L., Kumar, S. and Rehan, M., <i>On Vandermonde and MDS Rhotrices over $GF(2^q)$</i> , International Journal of Mathematics and Analysis, Vol. 5, No. 2, P. 143-160, (July- Dec., 2013).	0973-3604
16.	Sharma, P. L., Kumar, S. and Rehan, M., <i>On Hadamard Rhotrix over Finite Field</i> , Bulletin of Pure and Applied Sciences, Vol. 32 E (Math & Stat.), No.2, P. 181-190, (2013).	0970-6577
17.	Sharma, P. L. and Kumar, S., <i>Balanced Incomplete Block Design (BIBD) Using Hadamard Rhotrices</i> , International Journal of Technology, Vol. 4, No. 1, P. 62-66, (Jan.-June, 2014).	2231-3907

18.	Sharma, P. L. and Sharma, S. <i>An Application of Finite Field in Hill Cipher</i> , International Journal of Technology, Vol. 4, No. 1, P. 248- 251, (Jan.-June, 2014).	2231-3907
19.	Sharma, P.L. and Rehan, M., <i>Modified Hill Cipher Using Vandermonde Matrix and Finite Field</i> , International Journal of Technology, Vol. 4, No. 1, P. 252-256, (Jan.-June, 2014).	2231-3907
20.	Sharma P. L. and Kumar S., <i>Some applications of Hadamard rhotrices to design balanced incomplete block</i> , International J. of Math. Sci. & Engg. Appls. Vol. 8, No. II, P. 389-404, (March, 2014).	0973-9424
21.	Sharma P. L., Kumar S. and Rehan M. , <i>On construction of Hadamard codes using Hadamard rhotrices</i> , International Journal of Theoretical & Applied Sciences , Vol. 6, No. 1, P. 102-111(2014).	0975-1718
22.	Sharma P. L. and Rehan Mansi, <i>On approximate values of irreducible polynomials over $GF(3)$ with first three given coefficients</i> , International journal of Mathematics and analysis, Vol. 6, No. 1, P. 1-26, (January-June 2014),.	0973-3604
23.	Sharma P. L. and Rehan Mansi, <i>Approximating number of irreducible polynomials over $GF(p)$ with several given coefficients</i> , Bulletin of Pure and Applied Sciences, Vol. 33 E (Math & Stat.), No.1, P. 51-74, (2014).	0970-6577
24.	Sharma P. L. and Rehan Mansi, <i>On number of irreducible polynomials over finite field</i> , Recent Trends in Algebra and Mechanics, P. 41-56, Indo-American Books Publisher, New Delhi, (2014).	93-82661-23-9
25.	Sharma P. L. and Sharma Shabnam, <i>Sequences of irreducible polynomials over $GF(2)$ with three prescribed coefficients</i> , Recent Trends in Algebra and Mechanics, P. 21-32, Indo-American Books Publisher, New Delhi, (2014).	93-82661-23-9
26.	Sharma P. L. and Kumar Satish, <i>On a special type of Vandermonde rhotrix and its decompositions</i> , Recent Trends in Algebra and Mechanics, P. 33-40, Indo-American Books Publisher, New Delhi, (2014).	93-82661-23-9
27.	Sharma P. L., Sharma Shabnam and Dhiman Neetu, <i>Construction of infinite sequences of irreducible polynomials using Kloosterman sums</i> , Bulletin of Pure and Applied Sciences, Vol. 33 E (Math. & Stat.), No. 2, P. 161-168, (2014).	0970-6577
28.	Sharma P. L., Rehan M. and Sharma S., <i>Counting irreducible polynomials over $GF(3)$ with first and third coefficients given</i> , Asian-European Journal of Mathematics, Vol.8, No.1, 1550015(27 Pages),(2015).	1793-5571
29.	Sharma P. L. and Rehan Mansi. and Sharma Shabnam, <i>Irreducible polynomials over $GF(3)$ with first and second prescribed coefficients</i> , Asian Journal of Mathematics & Physics, Vol.2015, Article ID amp0209, 15 pages.	2308-3131

30.	Sharma P. L., Sharma S. and Rehan M., <i>On construction of irreducible polynomials over F_3</i> , Journal of Discrete Mathematical Sciences and Cryptography, Vol. 18, No. 4(2015), 335-347.	0972-0529
31.	Sharma P. L., Sharma Shabnam and Rehan Mansi , <i>Construction of Infinite Sequences of Irreducible Polynomials over F_2</i> , International Journal of Mathematical Sciences & Engineering Applications, Vol. 9, No. 3, September 2015.	0973-9424
32.	Sharma P. L., Kumar Satish and Rehan Mansi, <i>On Factorization of a Special Type of Vandermonde Rhoatrix</i> , Applications and Applied Mathematics: An International Journal (AAM), Vol.10, No.1, June 2015, 421-439.	1932-9466
33.	Sharma P. L. and Dhiman Neetu, <i>Generalization of Cross-correlation in Boolean Functions and Some Generalized Constructions in gbent Functions</i> , Asian-European Journal of Mathematics, Vol. 9, No.1(2016), 1650019 (7 pages).	1793-5571
34.	Sharma P. L. , Gupta Shalini and Rehan Mansi, <i>Construction of MDS Rhoatrices using Special Type of Circulant Rhoatrices over Finite Fields</i> , Himachal Pradesh University Journal (HPUJ), Vol. 3, No. 2(2015), pp. 25-43.	2277-1425
35.	Sharma P. L., Sharma Shabnam, <i>Hill Cipher Cryptosystem using Irreducible Polynomials over Finite Fields</i> , Himachal Pradesh University Journal (HPUJ), Vol. 3, No. 2(2015), pp. 44-52.	2277-1425
36.	Sharma P. L. and Devi Kiran, <i>An Elliptic Curve Cryptosystem over Finite Fields</i> , Himachal Pradesh University Journal (HPUJ), Vol. 3, No. 2(2015), pp. 1-12.	2277-1425
37.	Sharma P. L. and Dhiman Neetu , <i>A Characterization Theorem for gbent function over Z_{16}</i> , Journal of Combinatorics, Information & System Sciences (JCISS), Vol. 41, No. 1-3 (2016), pp. 47-55.	2277-1425
38.	Sharma P. L. and Devi Kiran, <i>A public key cryptosystem using normal bases over finite fields</i> , International Journal of Technology, Vol. 6(2), pp. 143-149, July-December, 2016.	2231-3907
39.	Sharma P. L. and Dhiman Neetu, <i>Some new constructions of gbent functions</i> , Bulletin of Pure and Applied Sciences Volume 35 E (Math & Stat.) Issue No.2 pp. 89-107, 2016.	0970- 6577

40.	Sharma P. L. and Dhiman Neetu, <i>Construction of a New Class of Bent and Semi-bent Functions</i> , International Journal of Computer Applications Vol. 157, No 2, pp. 9-12, 2017.	0975- 8887
41.	Sharma P. L. and Dhiman Neetu, <i>Construction of Some New Classes of Boolean Bent Functions and Their Duals</i> , International Journal of Algebra, Vol. 11, No.2, pp. 53 – 64, 2017.	1312-8868 (print) 1314-7595 (online)
42.	Sharma P. L., Sharma Shabnam, <i>On Identification of Irreducible Polynomials over Finite Fields with Characteristic P</i> , International J. of Math. Sci. & Engg. Appls. (IJMSEA) Vol. 11 No. I (April), pp. 19-35, 2017.	0973-9424
43.	Sharma P. L. and Devi Kiran, <i>A Secure Cryptosystem Based on Normal Bases over Finite Fields</i> , CPUH-Research Journal 2(2), pp.41-44, 2017.	2455-6076 (online)
44.	Sharma P. L., Sharma Shabnam and Kumar Arun, <i>A Symmetric Cryptosystem Based on Irreducible Polynomials over Finite Fields</i> , CPUH-Research Journal 2(2), pp.45-50, 2017.	2455-6076 (online)
45.	Sharma P. L. , Gupta Shalini and Rehan Mansi, <i>On Circulant-Like Rhotrices over Finite Fields</i> , Applications and Applied Mathematics: An International Journal (AAM), Vol. 12, No.1(June), pp. 506-520, 2017.	1932-9466
46.	Sharma P. L, Gupta Shalini and Dhiman Neetu, <i>Construction of Maximum Distance Separable Rhotrices using Cauchy Rhotrices over Finite Fields</i> , International Journal of Computer Applications, Vol.168, No.9, pp. 8-17, 2017.	0975-8887
47.	Sharma P. L., Gupta Shalini and Dhiman Neetu, <i>Sylvester Rhotrices and their Properties over Finite Fields</i> , , Bulletin of Pure and Applied Sciences, Vol. 36 E (Math. & Stat.), No. 1, pp. 70-80, 2017.	0970-6577 2320-3226 (online)
48.	Sharma P. L. and Gupta Shalini , <i>Constructions of Maximum Distance Separable Toeplitz Rhotrices over Finite Fields</i> , J. of Combinatorics, Information & System Sciences Vol. 42, No. 1-4, pp. 1-22, 2017.	2277-1425
49.	Sharma P. L. and Devi Kiran , <i>A class of Gaussian normal bases and their dual bases</i> , Journal of Discrete Mathematical Sciences and Cryptography, Vol. 20, No. 8, pp.1741-1755, 2017.	0972-0529
50.	Sharma P. L. and Devi Kiran, <i>Normal Elements using Trace Mapping over Finite Fields</i> , International Journal of Computer Applications, Vol. 179, No.20, pp.18-21, 2018.	0975–8887

51.	Sharma P. L. and Devi Kiran, <i>Finding Normal Bases Over Finite Fields Using Prescribed Trace Vectors</i> , International J. of Math. Sci. & Engg. Appls. (IJMSEA) Vol. 12, No. I, pp. 1-13, 2018.	0973-9424
------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------

[5] M.PHIL. STUDENTS GUIDED/ UNDER GUIDANCE:

Sr. No.	Name of Candidate	Title of Dissertation	Year	Status
1.	Sanjay Kumar	On Semirings with Decending Chain Condition and without Nilpotent Elements	2010	Completed
2.	Shabnam Sharma	On Finite Fields and Their Algebraic Properties	2011	Completed
3.	Minakshi	On RSA Algorithm in Cryptography	2011	Completed
4.	Neetu Dhiman	A Study of some Optimization Problems Related to the Moments	2012	Completed
5.	Paridhi Sharma	On the Discrete Logarithm Problem and Diffie- Hellman Algorithm in Cryptography	2012	Completed
6.	Kiran Thakur	On Primality Tests and Integer Factorisation Techniques	2013	Completed
7.	Kiran Devi	On Elliptic Curve Cryptography	2013	Completed
8.	Bhagat Ram	On Data Encryption Standard Algorithm in Symmetric Key Cryptography over Finite Field F_2	2014	Completed
9.	Neha	On ElGamal Cryptosystem and its Simulation using the Elliptic Curve over Finite Fields	2014	Completed
10.	Arun Kumar	On Digital Signatures using RSA Public Key Cryptosystem Scheme	2015	Completed
11.	Priyanka	On Cryptographic Hash Functions over the Finite Field with Characteristic 2	2015	Completed
12.	Ranjna Dilta	Design and Analysis of Some Stream Ciphers in Cryptography over the Finite Field F_2	2016	Completed
13.	Abhishek Thakur	Design and Analysis of Some Block Ciphers in Cryptography over the Finite Field F_2	2016	Completed
14.	Sweta Rana	Elliptic Curve Discrete Logarithm Problem in Cryptography	2017	Completed

15.	Nisha Rana	Elliptic Curve Digital Signature Algorithm in Cryptography	2017	Completed
16.	Dumita Kumari	Cryptography		Pursuing
17.	Nitish Kumar	Cryptography		Pursuing

[6] Ph. D. STUDENTS GUIDED / UNDER GUIDANCE :

Sr. No.	Name of Candidate	Title of Thesis	Year	Status
1.	Raj Kumar Kanwar	A Study of Some Analogous Properties of Rhotrices and Matrices	2013	Completed
2.	Satish Kumar	Extensions And Applications Of Vandermonde, Hadamard And Companion Rhotrices With Maximum Distance Separable Rhotrix Over Finite Field	2014	Completed
3.	Mansi Rehan	On Irreducible Polynomials over Finite Fields, their approximate number with some prescribed coefficients and Applications in Cryptography	2015	Completed
4.	Shabnam Sharma	On Irreducible Polynomials over Finite Fields, Their Infinite Sequences and Applications in Cryptography	2016	Completed
5.	Neetu Dhiman	On Constructions of New Classes of Bent, Semi-Bent and Generalized Bent Functions over Finite Fields	2017	Completed
6.	Shalini Gupta	Some new Rhotrices over Finite Fields and Constructions of Maximum Distance Separable Rhotrices	2017	Completed
7.	Kiran Devi	On Constructions of Normal Bases, Gaussian Normal Bases over Finite Fields and Their Applications in Cryptography	2017	Submitted
8.	Arun Kumar	Working on Symmetric key cryptography		Pursuing
9.	Anil Kashyap	Working on Elliptic curves over finite fields		Pursuing
10.	Gaurav Saini	Working on Finite Fields- Normal basis		Pursuing

**[7] DETAILS OF THE SEMINARS/CONFERENCE/WORKSHOPS /
REFRESHER COURSES ORGANISED:**

Sr. No.	Title of Conference	Period	Organising Institution	Capacity
1.	National Conference in Algebra	27-03-2012 To 28-03-2012	Department of Mathematics, Himachal Pradesh University, Shimla-5.	Organizing Secretary
2.	RC-254 (Refresher Course in Mathematics and Statistics)	16-07-2012 To 4-08-2012	ASC, H.P. University, Shimla-5.	Deputy Coordinator
3.	RC-265 (Refresher Course in Mathematics and Statistics)	24-06-2013 To 13-07-2013	ASC, H.P. University, Shimla-5.	Deputy Coordinator
4.	Advanced Instructional School on Diophantine Equations	16-06-14 To 04-07-14	Department of Mathematics, H. P. University, Shimla Sponsored by NCM Supported by NBHM	Coordinator
5.	National Instructional Workshop on Cryptology (NIWC-2015)	18-06-2015 To 22-06-2015	Department of Mathematics, H. P. Under the aegis of Cryptology Research Society of India (CRSI)	Coordinator
6.	National Conference on Algebra & Allied Fields	26-03-2016	Department of Mathematics, H. P. University, Shimla	Organising Chair
7.	National Seminar on Algebra & Allied Fields	24-25 March, 2017	Department of Mathematics, H. P. University, Shimla	Organising Chair

[8] ACADEMIC ASSIGNMENTS:

- (1) Life Member of “Cryptology Research Society of India (CRSI)”.
- (2) Life Member of “Indian Mathematical Society (IMS)”.
- (3) Life Member and Treasurer of “Himachal Mathematics Society (HIMS)”
- (4) Life Member of “The Indian Science Congress Association (ISCA)”.
- (5) Reviewer: American Mathematical Society (MathSciNet).