ARIZONA STATE UNIVERSITY

PROPOSAL TO ESTABLISH A NEW UNDERGRADUATE CERTIFICATE

The completed and signed proposal should be submitted by the Dean's Office to: curriculumplanning@asu.edu.
Before academic units can advertise undergraduate certificates or include them in their offerings as described in the university catalogs, they must be recommended for approval by the Senate Curriculum and Academic Programs Committee and the University Senate, and be approved by the Executive Vice President and Provost of the University.

Definition and minimum requirements:

These are the minimum requirements for approval. Individual undergraduate certificates may have additional requirements.

An undergraduate certificate is a programmatic or linked series of courses from a single field or one that crosses disciplinary boundaries and may be free-standing or affiliated with a degree program. The certificate provides a structured and focused set of courses that can be used to enhance a student's baccalaureate experience or professional development.

An undergraduate certificate program:

- Requires a minimum of 15 semester hours of which at least 12 semester hours must be upper division
- Requires a minimum grade of "C" or better for all upper division courses
- Consists of courses that must directly relate in whole or large part to the purpose of the certificate. Example: Geographic area certificates must include only courses specific to the title of the certificate, other than a non-English language
- Is cross disciplinary; or,
    - Certified by a professional or accredited organization/governmental agency; or,
    - Clearly leads to advanced specialization in a field; or,
    - Is granted to a program that does not currently have a major

College/School/Institute: College of Liberal Arts and Sciences

Department/Division/School: School of Mathematical and Statistical Sciences

Proposed Certificate Name: Cryptology

Requested effective Date: 2015-16

Delivery method: On-campus only (ground courses and/or iCourses)

Note: Once students elect a campus or On-line option, students will not be able to move back and forth between the on-campus and the ASU Online options. Approval from the Office of the Provost and Philip Regier (Executive Vice Provost and Dean) is required to offer programs through ASU Online.

Campus/Locations:
Indicate all locations where this program will be offered.

☐ Downtown Phoenix ☐ Polytechnic ☒ Tempe ☐ West Other:

Proposal Contact

Name: Nancy Childress **Title:** Assoc Director, SoMSS

Phone number: 480-965-3951 **Email:** nc@asu.edu

DEAN APPROVAL(S)

This proposal has been approved by all necessary unit and College/School levels of review. I recommend implementation of the proposed organizational change.

College/School/Division Dean name: Paul LePore

Signature ______________________ **Date:** / /20

College/School/Division Dean name:
(if more than one college involved)

Signature ______________________ **Date:** / /20

Note: An electronic signature, an email from the dean or dean's designee, or a PDF of the signed signature page is acceptable.

ARIZONA STATE UNIVERSITY

PROPOSAL TO ESTABLISH A NEW UNDERGRADUATE CERTIFICATE

1. Overview

A. Provide a brief description of the new certificate.
The Certificate in Cryptology is intended to develop students' expertise in the mathematics underlying modern cryptosystems. It is comprised of a combination of foundational courses on the mathematics needed to understand these cryptosystems, and specialized courses on the theory that explains the security they provide, the algorithms used to create and cryptanalyze them, and their potential vulnerabilities.

B. This proposed certificate (check one):

□ Is cross disciplinary; or

□ Is certified by a professional or accredited organization/governmental agency; or,

☒ Clearly leads to advanced specialization in a field; or,

□ Is granted to a program that does not currently have a major.

C. Why should this be a certificate rather than a concentration or a minor?
The proposed certificate program focuses on a highly specialized area. The knowledge it affords is deeper and more targeted than a minor or a concentration.

D. Affiliation
If the certificate program is affiliated with a degree program, include a brief statement of how it will complement the program. If it is not affiliated with a degree program, incorporate a statement as to how it will provide an opportunity for a student to gain knowledge or skills not already available at ASU.
There is, to our knowledge, no current degree program that focuses on mathematical cryptology. This certificate will provide ASU students interested in cryptology with in-depth knowledge of the mathematical theory behind it.

E. Demand
Explain the need for the new certificate (e.g., market demand, interdisciplinary considerations).
Used to protect personal, financial, proprietary, and defense-related information, cryptology is everywhere in today's technology. Modern cryptosystems are based on ideas from number theory, abstract algebra, and discrete mathematics. Individuals with expertise in these mathematical underpinnings are in high demand in private industries where information security is important, and in national security related careers. Our existing cryptology-related courses already attract a large number of students who regularly ask for opportunities for further study, and would be very interested in pursuing such a certificate. In addition, we anticipate that the proposed certificate will attract new students, including students from other majors who complete the certificate alongside their current degree programs, and post-degree students from industry who choose ASU specifically on account of this certificate.

F. Projected enrollment
What are enrollment projections for the first three years?

	1st Year	**2nd Year** (Yr. 1 continuing + new entering)	**3rd Year** (Yr. 1 & 2 continuing + new entering)
Number of Students (Headcount)	10	30	50

2. Support and Impact

A. Faculty governance

Provide a supporting letter from the chair of the academic unit verifying that the proposed certificate has received faculty approval through appropriate governance procedures in the unit and that the unit has the resources to support the certificate as presented in the proposal, without impacting core program resources.

attached

B. Other related programs

Identify other related ASU programs and outline how the new certificate will complement these existing ASU programs. (If applicable, statements of support from potentially-affected academic unit administrators need to be included with this proposal submission.)

C. Letter(s) of support

Provide a supporting letter from each college/school dean from which individual courses are taken.

3. Academic Curriculum and Requirements

A. Knowledge, competencies, and skills

List the knowledge, competencies, and skills (learning outcomes) students should have when they complete this proposed certificate. Examples of program learning outcomes can be found at (http://www.asu.edu/oue/assessment.html).

Students will be able to describe precisely the steps involved in implementing the most widely used contemporary cryptosystems, and explain the mathematical theory behind the purpose of these steps.

Students will be able to explain the theoretical reasons for known vulnerabilities in contemporary cryptosystems, describe how known attacks are carried out, assess the likelihood a given attack succeeds, and explain how it can be thwarted.

Students will be able to describe precisely the steps performed in contemporary factorization and discrete log algorithms and assess the efficacy of each algorithm.

Students will be able to use theoretical concepts from number theory, group theory, discrete mathematics, probability and/or statistics to assess proposed cryptosystems for practicality and security.

B. Admissions criteria

List the admissions criteria for the proposed certificate. If they are identical to the admission criteria for the existing major and degree program under which this certificate will be established, please note that here.

ASU student in good academic standing with B- or better in MAT 300 or equivalent

C. Curricular structure

Provide the curricular structure for this certificate. Be specific in listing required courses and specify the total minimum number of hours required for the certificate.

Required certificate courses

Prefix	Number	Title	Is this a new Course?	Credit Hours
MAT	440	Group Theory*	Yes	3
MAT	445	Theory of Numbers	No	3
MAT	447	Cryptography I	No	3
MAT	448	Cryptography II	Yes	3
			Section sub-total:	12

* MAT 444 Intermediate Abstract Algebra can be substituted for MAT 440

Elective certificate courses

Prefix	Number	Title	Is this a new Course?	Credit Hours
MAT	415	Introduction to combinatorics	No	3
MAT	416	Introduction to GraphTheory	No	3
MAT	441	Ring Theory	Yes	3
STP	421	Probability	No	3
STP	427	Mathematical Statistics	No	3
			Section sub-total:	6

Note: Three credits of cryptology related Internship (MAT 484) can be substituted for an elective course

	Credit Hours
Other certificate requirements	
E.g. – Capstone experience, internship, clinical requirements, field studies, foreign language skills as applicable	
Section sub-total:	0
Total minimum credit hours required for certificate	**18**

D. Minimum residency requirement

How many hours of the certificate must be ASU credit? 18

E. New Courses
Provide a brief course description for each new course.

MAT 440 Group Theory (3) This course covers basic group theory. Students will learn about the concept of a "group," related structures, their underlying theory, and examples of how they arise in mathematics.

MAT 441 Ring Theory (3) This course covers the basic ring theory. Students will learn about the concept of a "ring,"related structures, their underlying theory, and examples of how they arise in mathematics.

MAT 448 Cryptography II (3) This course is a continuation of Cryptography I. Students will learn about the mathematical underpinnings of contemporary cryptosystems, electronic signatures, key exchange, primality testing, and factorization algorithms.

Note: All new required courses should be submitted in Curriculum ChangeMaker and ready for Provost's Office approval before this certificate is put on Curriculum and Academic Programs Committee (CAPC) agenda.

4. Administration and Resources

A. Administration
How will the proposed certificate be administered (including admissions, student advisement, retention, etc.)?
Professor Nancy Childress will act as administrator of this certificate, with support from the SoMSS advising staff.

B. Resources
What are the resource implications for the proposed certificate, including any projected budget needs? Will new books, library holdings, equipment, laboratory space and/or personnel be required now or in the future? If multiple units/programs will collaborate in offering this certificate please discuss the resource contribution of each participating program. Letters of support must be included from all academic units that will commit resources to this certificate.

Existing resources within SoMSS will suffice.

C. Primary Faculty
List the primary faculty participants regarding this proposed certificate. For interdisciplinary certificates, please include the relevant names of faculty members from across the University.

Name	Title	Area(s) of Specialization as they relate to proposed certificate
Andrew Bremner	Professor	Number Theory, Algebra, and Cryptography
John Jones	Professor	Number Theory, Algebra, and Cryptography
Nancy Childress	Assoc Director, Assoc Professor	Number Theory, Algebra, and Cryptography

5. Additional Materials

A. Complete and attach the Appendix document.

B. Provide one or more model programs of study (if appropriate).

C. Attach other information that will be useful to the review committees and the Office of the Provost.

APPENDIX

OPERATIONAL INFORMATION FOR UNDERGRADUATE CERTIFICATES

(This information is used to populate the Degree Search/catalog website.

Please consider the student audience in creating your text.)

A. **Proposed Certificate Name:** Cryptology

B. **Description (150 words maximum)**
The certificate in cryptology is designed to provide a strong foundation in the mathematical topics that are most applicable to modern cryptosystems. It also provides specialized knowledge required to understand and work in the field of mathematical cryptology.

C. **Contact and Support Information**

Building Name, code and room number: *(Search ASU map)*	PSA 211
Program office telephone number: (*i.e. 480/965-2100*)	480/965-7195
Program Email Address:	math@asu.edu
Program Website Address:	http://math.asu.edu

D. **Program Requirements:** Provide applicable information regarding the program such as curricular restrictions or requirements, specific course lists, or academic retention requirements.
This certificate requires 18 credit hours.

Required courses:
MAT 440 Group Theory* (3)
MAT 445 Theory of Numbers (3)
MAT 447 Cryptography I (3)
MAT 448 Cryptography II (3)
* may substitute MAT 444 Intermediate Abstract Algebra for MAT 440

Electives (select two from the following list)**
MAT 415 Introduction to Combinatorics (3)
MAT 416 Introduction to Graph Theory (3)
MAT 441 Ring Theory (3)
STP 421 Probability (3)
STP 427 Mathematical Statistics (3)
** may substitute three credit hours of approved crypology-related internship experience (MAT 484) for one elective

E. **Additional Admission Requirements** If applicable list any admission requirements (freshman and/or transfer) that are higher than and/or in addition to the university minimum undergraduate admission requirements.)
This program has additional admission requirements. Applicants should be in good academic standing with "B"or better in MAT 300 Mathematical Structures (3) or equivalent.

F. **Delivery/Campus Information Delivery:** On-campus only (ground courses and/or iCourses)

Note: Once students elect a campus or On-line option, students will not be able to move back and forth between the on-campus and the ASU Online options. Approval from the Office of the Provost and Philip Regier (Executive Vice Provost and Dean) is required to offer programs through ASU Online.

G. **Campus/Locations:**
Indicate **all** locations where this program will be offered.
☐ Downtown Phoenix ☐ Polytechnic ☒ Tempe ☐ West Other:

Julie Ramsden

From: Paul LePore <Paul.Lepore@asu.edu>
Sent: Thursday, April 10, 2014 10:46 AM
To: curriculumplanning@asu.edu
Cc: Jenny Smith; Paul LePore
Subject: Proposal to establish a new undergraduate certificate in Cryptology
Attachments: Crypto Proposal rev. 4-8-14.doc; crypto memo.pdf

Please accept the attached proposal to create a new undergraduate certificate in Cryptology.

Thank you.

PL

PAUL C. LEPORE, Ph.D.
Associate Dean
College of Liberal Arts and Sciences
Foundation Building, Suite 110
Arizona State University | P.O. Box 876605 | Tempe, Arizona 85287-6605
480.965.6506 | Fax: 480.965.2110 | e-mail: paul.lepore@asu.edu

ASU College of Liberal Arts and Sciences — *Transforming learning, discovery and lives*

ASU SCHOOL OF MATHEMATICAL & STATISTICAL SCIENCES

ARIZONA STATE UNIVERSITY

February 17, 2014

To Whom it May Concern:

With this memorandum, I give my strong support for the proposed certificate program in Cryptology.

Cryptologists use their knowledge of mathematics to devise, improve, or break encryption algorithms intended to protect private information. In addition to traditional defense-related applications, cryptology has become increasingly important in private industry, as communication systems, electronic banking, electronic health records, and internet commerce continue to expand.

Particularly relevant for contemporary cryptologic applications are the mathematical fields of number theory, abstract algebra, discrete mathematics, probability, and statistics. Existing SoMSS courses in these areas already attract students interested in cryptology. Requests for a deeper and more focused program of study in cryptology are common, and such a program would better prepare students for cryptology-related careers.

The certificate program received unanimous approval by our undergraduate program committee. As per our by-laws, this is the committee charged with reviewing degree programs, new course proposals, and curriculum changes at the undergraduate level.

Our school has three current faculty members with cryptology expertise. We anticipate no impact to any core programs with the school.

Please let me know if you have any additional questions regarding my support of this certificate.

Sincerely,

Al Boggess, Director