Saint Vincent College

**Quality Education in the Benedictine Tradition**

**Applied Cryptography**

CS 375

Fall 2019

* 3 credits
* Prerequisites: CS 170, CS 221
  + Students should have both a good math and programming background.
* Instructor: [Brother David Carlson](https://cis.stvincent.edu/cis/FacultyInfo/BrDavid.php)
* Office: Dupre Science Pavilion, Tenley Hall W217
* Office hours:
  + Mon, Wed, Fri 9:30 am - 11:20 am
  + Mon, Fri 2:00 pm - 2:50 pm
  + Tue 1:00 pm - 2:30 pm
  + Thurs 8:30 am - 11:20 am
  + and by appointment
* Phone: 724-805-2416
* Email: [david.carlson@stvincent.edu](mailto:david.carlson@stvincent.edu)
* Class Times and Location
  + Mon, Fri 12:30 pm - 1:45 pm, Dupre W214
* Date of Final Exam
  + Tue, Dec 10, 4:00 pm - 6:00 pm

**Course Description**

This course presents sufficient number theory and algebra to describe common cryptographic systems. Course topics include the German Enigma machine, DES, AES, the RSA cryptosystem, discrete logarithms, the ElGamal cryptosystem, elliptic curve cryptography, quantum cryptography, and possibly others. The mathematics behind cryptography, such as number theory and finite fields, will also be studied. Students will use computer software to solve cryptography problems and will write their own software to handle some types of cryptography, cryptanalysis, etc. Mathematica may be used to solve some of the problems. Students will be asked to implement several cryptographic algorithms using C++ in Linux with the aid of the BigInt package. Some of these algorithm implementations might be done as group projects. Common applications of cryptography such as key distribution, digital signatures, user authentication, and network security will also be studied, as well as some of the methods of attacking cryptosystems.

**Required Course Books and Other Materials**

Text: Cryptography and Network Security: Principles and Practice, 7th ed., Stallings, W., Pearson Education (2017), ISBN 9780134444284. Either the printed text or the e-book can be used as exams are closed book in this course.

**Relevant CIS Department Student Learning Outcomes**

By the time of graduation

|  |
| --- |
| 1. The CS, IS, or CYSEC major will have an ability to analyze a complex computing problem and apply principles of computing and other relevant disciplines to identify solutions. 2. The CS, IS, or CYSEC major will have an ability to design, implement, and evaluate a computing-based solution to meet a given set of computing requirements in the context of the program’s discipline. 3. The CS, IS, or CYSEC major will have an ability to recognize professional responsibilities and make informed judgments in computing practice based on legal and ethical principles. 4. The CS major will have an ability to apply computer science theory and software development fundamentals to produce computing-based solutions. 5. The CYSEC major will have an ability to apply security principles and practices to maintain operations in the presence of risks and threats. 6. The CS, IS, or CYSEC major will have an ability to reason about and explain computer-based solutions at multiple levels of abstraction. |

**Course Learning Objectives**

By the end of the course, students will be able to:

|  |
| --- |
| 1. Explain and trace the operation (both in the software code and in mathematics) of each cryptographic algorithm, protocol, and application that was studied in detail. This supports student learning outcome 6 above. 2. Design, modify, complete, and add to cryptographic software. This supports student learning outcomes 1, 2, and 4 above. 3. Carry out cryptanalysis and other attacks against cryptosystems, explaining the results and suggesting improvements to the cryptosystems based on these results. This supports student learning outcomes 5 and 6 above. 4. Explain the tradeoffs and any legal or ethical concerns among competing cryptographic methods, applications, and activities. This supports student learning outcome 3 above. |

**Course Schedule**

Note that the assignment questions numbered in the format n.m are in the Problems section (not the Review Questions section) at the end of each chapter. Due dates are posted in Schoology. The schedule below merely attaches assignments to the correct spot in the course.

|  |  |  |
| --- | --- | --- |
| Date | Topic | Assignment/Exam |
| Wk 1, Aug 26 | Syllabus, Ch 1: Overview, xor as simple encryption | HW 1: cryptanalysis with cryptoquotes |
| Wk 1, Aug 30 | Frequency-based cryptanalysis with cryptoquotes, cryptanalysis with xor | HW 2: cryptanalysis with 1-time pad (xor) |
| Wk 2, Sept 2 | Labor Day: no class |  |
| Wk 2, Sept 6 | Ch 2: Number theory, cryptanalysis section of IntroCryptographyCryptanalysis.pdf | HW 3: extended Euclidean algorithm |
| Wk 3, Sept 9 | Ch 2: Number theory, Cryptanalysis.docx | HW 4: problems 2.3, 2.10, and solve the 2 congruences |
| Wk 3, Sept 13 | Ch 2: Number theory, legal issues for cryptographic products | HW 5: problems 2.20, 2.22, 2.24, 2.32, 2.37a |
| Wk 4, Sept 16 | Ch 2: Number theory, bigint software for finding primes and doing number theory | HW 6: Chinese remainder theorem & discrete log problems |
| Wk 4, Sept 20 | Ch 2: Number theory, Ch 3: Breaking the enigma machine, role of Alan Turing, symmetric model, Enigma.docx, CodeBreakingWW2.doc, EnigmaCryptanalysis.pdf, TuringBombe.pdf | HW 7: enigma and Turing |
| Wk 5, Sept 23 | Ch 3: Substitution & transposition, more on bigint software for finding primes and doing number theory | HW 8: modification to bigint software to get probable primes, use Mathematica to multiply them and factor the product |
| Wk 5: Sept 27 | Ch 4: DES, breaking DES, monkey-in-the-middle attacks, extra chapter on DES details along with linear and differential cryptanalysis: Z22\_STAL4284\_07\_SE\_APPS\_DES.pdf | HW 9: write bigint software to do modular exponentiation, find primitive roots |
| Wk 6: Sept 30 | Ch 5: Finite fields,  DESAlgorithmIllustrated.docx | HW10: problem 4.2 and the problems in DES\_Homework.docx |
| Wk 6: Oct 4 | Ch 5: Finite fields | HW 11: 5.2, 5.4, 5.7, and one polynomial arithmetic problem |
| Wk 7: Oct 7 | Can cover anything done in the course thus far. | Midterm exam |
| Wk 7: Oct 11 | Ch 6: AES, KoolSpanSuiteBAlgorithms.docx,  EvalCritereaAES.pdf | HW 12: 6.5, 6.7, 6.11 |
| Wk 8: Oct 14 | Fall break: no class |  |
| Wk 8: Oct 18 | Ch 7: Block cipher operation, Ch 8: Random bit generation & stream ciphers, FIPS140.pdf, NIST.FIPS.140-2.pdf | HW 13: 7.4, 7.5, 7.8, 8.1, 8.4, 8.9ab |
| Wk 9: Oct 21 | Ch 9: RSA | HW 14: finish RSA encryption/decryption software in bigint |
| Wk 9: Oct 25 | Ch 9: RSA, engineering it, breaking it, software for RSA | HW 15: complete the bigint code to attempt to break RSA by factoring n as the difference of 2 squares |
| Wk 10: Oct 28 | Ch 10: Diffie-Hellman key exchange and monkey-in-the-middle attacks, youngblood\_csep590tu\_final\_paper.pdf | HW 16: 10.2, 10.5 |
| Wk 10: Nov 1 | Ch 10: ElGamal cryptosystem | HW 17: 10.6 |
| Wk 11: Nov 4 | Ch 10: ElGamal cryptosystem, software for ElGamal | HW 18: 10.12, 10.13 |
| Wk 11: Nov 8 | Ch 10: Breaking ElGamal |  |
| Wk 12: Nov 11 | Ch 10: Elliptic curve cryptography | HW 19: Elliptic curve cryptography software and 10.13 |
| Wk 12: Nov 15 | Ch 11: Cryptographic hash functions & birthday attacks, cse484-lecture\_Authenticataion-yoshi.pdf, StoringPasswordsSafely.docx | HW 20: finish "birthday attack" program and use it to look for collisions for a hash function |
| Wk 13: Nov 18 | Quantum cryptography, Ch 12: Message authentication codes, IntroductionToQuantumCryptography.docx and QuantumCryptoCSOOnline.docx, SchneierOnQuantumResistantCrypto.docx | HW 21: 12.9 |
| Wk 13: Nov 22 | Ch 13: Digital signatures, Ch 14: Key management & distribution | HW 22: 13.2, 13.3, 14.3, 14.5 |
| Wk 14: Nov 25 | Ch 15: User authentication, Ch 16: Network access control & cloud security, PostQuantumCrypto.docx | HW 23: 15.3, 15.4, 15.5 |
| Wk 14: Nov 29 | Thanksgiving break: no class |  |
| Wk 15: Dec 2 | Ch 17: Transport-level security, Ch 18: Wireless network security | HW 24: 17.3, 17.5, 18.2 |
| Wk 15: Dec 6 | Ch 19: Electronic mail security, ethics & cryptography, ImplementationFailures.pdf, review | HW 25: 19.4, 19.7 |
| Finals Week: Dec 10 | Covers mostly topics from after the midterm exam, but a few questions from the first half of the course will be included. | Final exam, 4:00 - 6:00 pm |

**Course Requirements and Grading**

|  |
| --- |
| * 34% Homework (includes the software projects mentioned in the course schedule) * 33% First Exam * 33% Final Exam * If the student does not attain a passing average in the test category, a failing grade will be received for the course |
| Letter grades will be given using the scale found in the College Bulletin. Exams will be announced in advance and will be closed-book, pencil and paper exams in nature, except that you may use two two-sided 8.5 in. x 11 in. pages of notes of any kind. Thus, on exams, only the test paper, calculators, the two pages of notes, pens, pencils, and erasers may be used. Cell phones, tablets, laptops, and similar devices should be turned off and put away. Calculators may be used on exams but are not to be shared among students.  All written work is expected to be done using good English and mathematics. This is intended to help the student to develop good written communications skills. Software assignments will be graded using the following rubric:   |  | | --- | | * 45% Correctness (meets its specifications) * 15% Good program design * 15% Clarity, style, and readability * 15% Good documentation * 10% Efficiency | |

Tests will ask critical thinking questions that require careful analysis, explanation, and sensible conclusions. You might be asked to solve a problem that requires some mathematics, to write a section of code, to analyze a security issue, etc. Homework will be of various types. Some will be programming projects, others will be experiments using existing software, and others might require some analysis or problem-solving using mathematics, computer science, or security principles. Watch Schoology for details of assignments, their due dates, etc.

Exam questions normally require you to show all major steps for producing the answer to each question. Failure to do so will likely result in losing a significant number of points on the problem. It is more important to know how to solve a problem and explain it well than to simply have the correct answer. Exceptions where you can simply write the answer will be marked.

Make-up exams are discouraged. If possible, take the regularly scheduled exam. For an excused absence or other significant reason, the instructor will likely agree to give a make-up exam. Whenever possible, see your instructor ahead of time if you know you must miss an exam (e.g. due to sports). Normally some type of written documentation is required (such as a note from the coach, doctor, etc.). If the documentation or reason for missing an exam is poor, the student can count on receiving a significantly more difficult exam, if one is given at all! Do ask about a makeup exam if you have a good reason to miss an exam, even if documentation is not readily available, as it is understood that illnesses and other complications do happen. Students participating in sports teams are required to notify the instructor in advance of games that might conflict with class.

**Course Policies**

*Academic Honesty Policy*

Saint Vincent College assumes that all students come for a serious purpose and expects them to be responsible individuals who demand of themselves high standards of honesty and personal conduct. Therefore, it is college policy to have as few rules and regulations as are consistent with efficient administration and general welfare. Fundamental to the principle of independent learning and professional growth is the requirement of honesty and integrity in the performance of academic assignments, both in the classroom and outside, and in the conduct of personal life. Accordingly, Saint Vincent College holds its students to the highest standards of intellectual integrity and thus the attempt of any student to present as his or her own any work which he or she has not performed or to pass any examinations by improper means is regarded by the faculty as a most serious offense. In any case of academic dishonesty, the faculty member together with the Assistant Vice President for Student Success and Retention, who confers with the student, decide on the appropriate sanction. Depending on the seriousness of the offense, possible sanctions are failure for the assignment, failure for the course, suspension or expulsion. If a student receives the sanction of a failure for the course during the withdrawal period and drops the course, a WF will be recorded on the transcript.

In this course, students are expected to do entirely their own work on the exams and homework. (A possible exception is that students may be asked to work in small groups on some of the software homework.) Every assignment should list all sources that contributed to the solution. This would include the individual student (or the group members if we do a small group software project). It may also include the instructor, a reference book, a web site, etc. Web sites or people that simply give you a solution to an assignment are not to be used. One student or group should not consult another student or group in the class. If you need assistance beyond simple clarification of the description of the assignment, consult the instructor. You may not look at the work of another student (or group) in this course or show yours (even a part of it) to another student (or group) in the course. You may not work out an assignment with one or more other students from the course (who are not in your group, for a group project). If you break one of the conditions spelled out in the last two sentences, then this is a case of **academic dishonesty**. See above for how this gets handled and the possible consequences.

*Attendance Policy*

* If the student does not attain a passing average in the test category, a failing grade will be received for the course.
* Each unexcused class absence after the first 3 results in 1.5 percentage points being deducted from the final course grade.
* Arriving late for class or leaving early (without a proper excuse) is counted as 1/2 of an absence.
* An unexcused absence from an exam results in the failure of the course.
* Unexcused absence from more than one-third of the semester's classes results in the failure of the course.
* Attendance is used to decide borderline grades at the end of the semester.
* Late work is not accepted unless resulting from an excused absence, but partial credit is given for incomplete homework that is submitted on time.
* Email me if you must miss class for any reason, whether it is due to an illness or some other issue. It is always best to let me know instead of leaving me to wonder why you are not in class.
* Written documentation (such as a note from a doctor's office or coach of one's sports team) is normally required for an absence to be excused. Always bring a copy of such a note to give to your instructor when you can do so. In special circumstances, check with your instructor, as it is not always possible to get documentation.
* Note on flu:
  + Because of the possibility of the flu affecting us on campus, please practice good hand washing, etc. If you get the flu, please notify me by phone or e-mail and stay home for 24 hours after the fever has gone. Check with me about what you miss. You will not be penalized for missing class in this situation. It is better to stay away from class and not spread the flu when you are ill.

*Class Cancellation Policy*

If the instructor needs to cancel class, every effort will be made to send an email message to students' Saint Vincent email accounts.

*Classroom Etiquette*

An essential characteristic of Saint Vincent College is the dignity and civility with which students and instructors conduct themselves both inside and outside the classroom. All students share in the responsibility of making the classroom a positive place to learn. Attendance is more than just being in the classroom, laboratory or field experience. Students are expected to be prepared and attentive. Some specific behaviors that are distracting and should be avoided include holding side conversations, arriving late or leaving early, doing work for other classes, eating, or using laptops to check email or surf the web. Cell phones, pagers, and other electronic devices must be turned off when students are in the classroom, labs, or when meeting with a faculty or staff member unless specific permission has been given by the instructor. Students should check with individual professors for additional expectations and guidelines for classroom etiquette, including whether or not tape recording of classroom lectures is permitted.

On a practical level, strive to do well in the course: read the text, attend class, do the work, ask questions, and try to answer questions in class! Mathematics, computer science, and cybersecurity are not spectator sports! They require active participation and repeated practice. If you begin to feel lost, consult one of the tutors, see the instructor, or work through the difficulties with the help of another student in the course. Do not let yourself get behind. In fact, one key to academic success is to start early on homework and other tasks. Last-minute miracles seldom work! Note in particular that attendance is expected. Student performance is bound to deteriorate when classes are missed.

*Accommodations for Disability*

Students with disabilities who may be eligible for academic accommodations and support services should contact Ms. Marisa Carlson, Assistant Dean of Studies, by phone (724-805-2828), email (marisa.carlson@stvincent.edu) or by appointment (Academic Affairs-Headmasters Hall). Reasonable accommodations do not alter the essential elements of any course, program or activity. The Notification of Approved Academic Accommodations form indicates the effective date of all approved academic accommodations and is not retroactive.     

**Title IX Statement**

Saint Vincent faculty are committed to helping create a safe learning environment for all students and for the college as a whole. If you have experienced any form of gender or sex-based discrimination or harassment, including sexual assault, sexual harassment, intimate partner (dating or domestic) violence, sexual exploitation, or stalking, know that help and support are available. Saint Vincent College has staff members trained to support students in navigating campus life, accessing health and counseling services, providing academic and housing accommodations, and more. The College strongly encourages all students to report any such incidents.

Please be aware that all Saint Vincent employees (other than those designated as confidential employees such as counselors, clergy and healthcare providers) are required to report information about such discrimination and harassment. This means that I have a mandatory duty to report to the Title IX Coordinator any information I receive about possible sexual misconduct.  This includes information shared in class discussions or assignments, as well as information shared in conversations outside class.  The Title IX Coordinator will contact you to inform you of your rights and options and connect you with support resources, including possibilities for holding accountable the person who harmed you. Know that you will not be forced to share information and your level of involvement will be your choice. The purpose of reporting is to allow Saint Vincent to take steps to ensure that you are provided with any necessary resources needed and to provide a safe learning environment for all.

The College’s Title IX Coordinator is:

Eileen K. Flinn, Esq.

Saint Vincent College

Second Floor, Alfred Hall

724-805-2897

The College also has confidential resources available, who can provide assistance to those who have experienced sexual misconduct without triggering a mandatory reporting duty.  More information about confidential resources is available at <https://www.stvincent.edu/student-life/title-ix>.

If you wish to speak to a confidential employee who does not have this reporting responsibility, you can contact Campus Ministry at 724-805-2350 or the Wellness Center in the Carey Student Center at 724-805-2115. For more information regarding your rights and options, please see the Sexual Misconduct and Harassment policy which can be found on MySVC portal under Quick Links or on the web at <https://www.stvincent.edu/student-life/title-ix>.