

# Alexander Scheel

Alexander Maurice Scheel  
alexander.m.scheel@gmail.com  
8192-bit RSA Key

6610 Kristin LN NW  
Rochester, MN 55901  
C: (507) 206-8310

GitHub – cipherboy  
Pagure – cipherboy

## [Overview]

- Interested in academic research, algorithm, protocol, and application development.
- Algorithmic specialties include graph theory, cryptography, and boolean satisfiability.
- Research interests include hash functions, post-quantum cryptography, and formal methods.

## [Education]

### Iowa State University (2015 – present)

- Honors Project: Collisions in Hash Functions (see below)
- Majors: Computer Science and Mathematics
- Classification: 3rd Year
- Dean's List: Fall 2015, Spring 2016, Fall 2016, Spring 2017
- Expected graduation: Spring 2018
- Credits: 131 (Senior)    • GPA: 3.8

## [Research Experience]

### Collisions in Hash Functions    March 2017 – present

- Research under Dr. Eric Rozier.
- Modeling collisions in hash functions as 3-CNF-SAT problems.
- Deriving metrics of utilities of collisions to evaluate impact of a collision.
- Analyzing breadth of collision malleability.
- Improving bounds for second preimage attacks.
- Contributing to [open access](#) and [open source](#) research.

## [Awards & Events]

### Awards

#### ACM ICPC – North Central North America region

- Fall 2017: 1st in site, 4th place overall
- Competed in Fall 2015 and Fall 2016

#### ΦBK Junior Inductee, Spring 2017

### ISEAGE Cyber Defense Competitions

- ISU CDC: 5th place – Fall 2016
- ISU CDC: 4th place – Spring 2016
- National CDC: 1st place – 2016
- ISU CDC: 2nd place – Fall 2015

### Events:

- [HackISU](#) – Fall 2015

## [Work Experience]

### Red Hat – Identity Management    June 2017 – August 2017

- Focused on enabling [Channel Bindings](#) in MIT Kerberos.
- Over 20 accepted pull requests across MIT Kerberos, gssproxy, ding-lib, python-gssapi, and libverto.
- Contributed to improving Kerberos interactions with SSH and NFS (Red Hat Bugzilla [#1199363](#), [#1477231](#), and [#1463665](#)).

### ISEAGE    October 2016 – present

ISEAGE is a security research lab at ISU which runs five Cyber Defense Competitions a year under the direction of Dr. Doug Jacobson.

- Developed scenario VM images, exploitable backdoors, and competition anomalies for use in an isolated environment.
- Competition roles include Red Team (volunteer hackers) Lead and Green Team (usability testing) Lead.
- Multiple responsibilities including lab leadership, sponsorship activities, and infrastructure development.

### IBM Cloud Managed Services    May 2016 – August 2016

CMS is a portion of IBM providing managed services on top of a diverse cloud platform for hundreds of companies.

- Automated compliance and security; improved developer workflow and auditing of compliance with Nessus and AppScan on Source in Java.
- Technical mentorship under Steven J. Munroe. Optimizations for SHA-3 on Power8+ assembly with vector instructions.

#### [Rochester Clinic](#) 2014–2015

**Rochester Clinic** is a family owned clinic based in Rochester, Minnesota.

- Software and hardware consultant.
- Lead patient data migration of 12k records to a new EMR provider. Database manipulation and CSV generation using Ruby, implemented [C-CDA](#) from specification, XSLT rendering. Education of staff regarding migration procedures.

#### [Projects]

##### [Cryptopals](#) present

Solving various cryptographic challenges and attacking insecure assumptions. Completed 54 out of 56 problems.

##### [COMS 309 – EduTLS](#) 2016

TLS 1.2 library implemented in C++ as part of an API-based web framework.

##### [crypto-collection](#) present

Various cryptographic algorithms with cross-platform implementations in C.

#### [Technology]

##### Programming Languages:

C, Java, Python, Go, Ruby, XML/HTML5, CSS3, JavaScript, PHP, C++, Assembly

Operating Systems: Fedora, Mac OS X, Windows

Project Management: Git, [GitHub](#), [Pagure](#), Make

Protocols and Encodings: TLS, Kerberos, ASN.1

**References available upon request.**