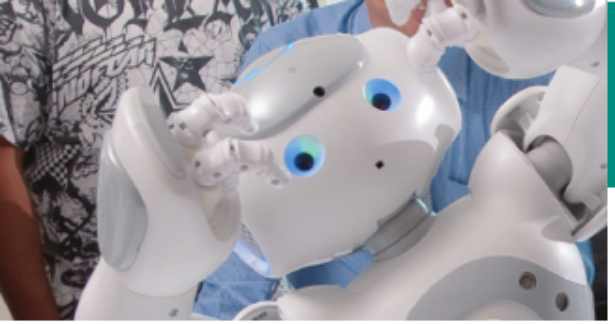
Dr. Melissa Danforth

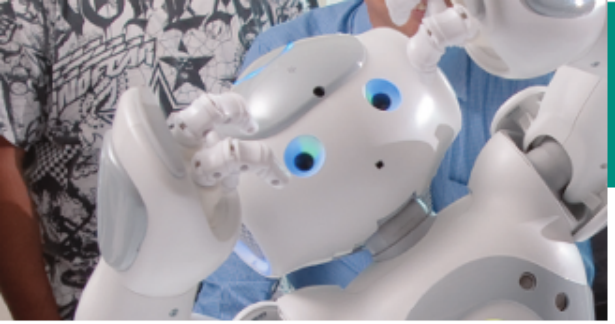
Dr. Charles Lam

Four Week Summer Program in Cyber Security for High School Students



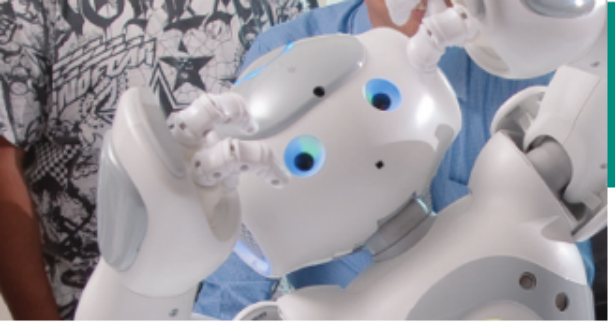
Overview

- Hands-on, intensive program during summer
  - Mid-July to early August
  - Four days each week (Mon. – Thurs.)
  - Six hours each day, including breaks
- Focused on cyber security
  - Cryptography (Charles Lam)
  - Network/Computer Security (Melissa Danforth)



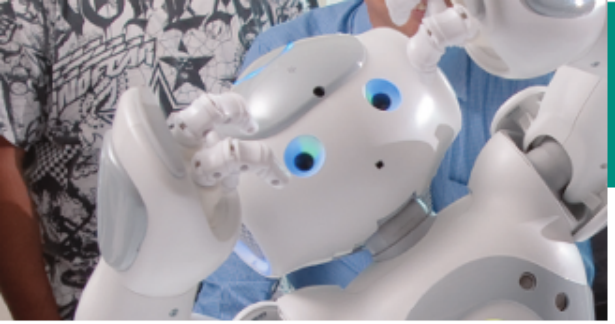
Cryptography Schedule

- Week 1
  - Substitution ciphers, Euclidean algorithm, Modular arithmetic
- Week 2
  - Fermat's Little Theorem, Modular exponentiation algorithm, RSA encryption
- Weeks 3 & 4
  - Work on hands-on project & prepare poster



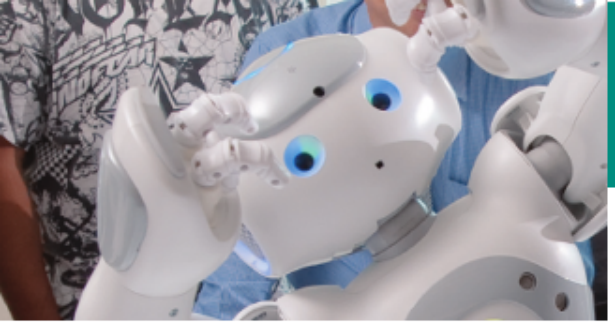
Cryptography Projects

- Students used knowledge gained in first two weeks to develop a project in cryptography
- Students developed three projects
  - Fact-or Fiction (factoring and its effects on RSA)
  - Elliptic Enigma (elliptic curve cryptography)
  - Zero Knowledge, We Know Everything (zero knowledge protocols)



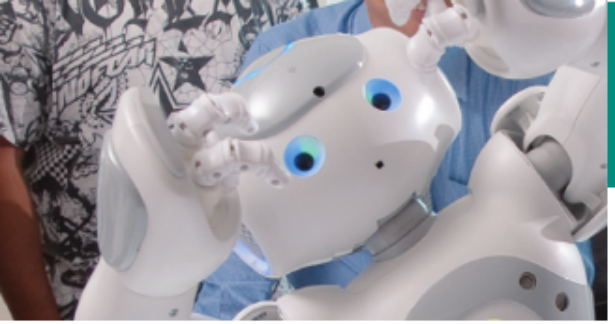
General Security Schedule

- Week 1
  - Ethics and legality (reinforced throughout), security principles, authentication, passwords, password cracking, how to use Linux/CLI
- Week 2
  - Passwords continued, secure authentication, network attacks, social engineering
  - Start projects: primarily in the afternoon



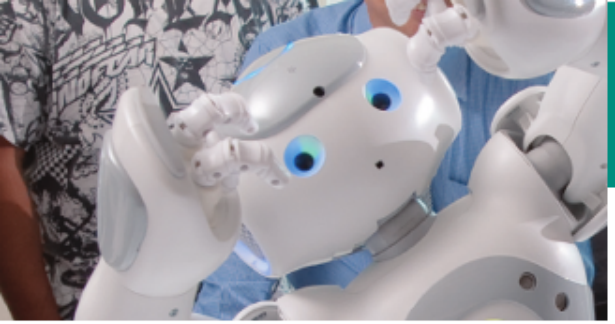
Security Schedule Continued

- Week 3
  - Social engineering continued, malware, access control, protecting information, best practices
  - Continue working on projects
- Week 4
  - Watch videos on recent security topics
  - Prepare posters, print posters, practice for poster competition



General Security Projects

- Students spent the afternoon of Week 2 and most of Week 3 on projects
- Students developed two projects
  - Crack Me if You Can: Using GPU Machines to Crack Passwords
    - Highest placing Mathematics/Engineering/Computer Science poster in the poster competition
  - Defense Against Human Hacking (social engineering)



Conclusion

Lecture notes, presentations, worksheets, activities, and posters are available at

http://www.cs.csub.edu/~melissa/revs-up/

Disclaimer: Partial support for this work was provided by the National Science Foundation's Federal Cyber Service: Scholarship for Service (SFS) program under Award No. 1241636. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.