A Cyber Security Discovery Program: Hands-on Cryptography

Abdullah Konak
Information Sciences and Technology
Penn State Berks
Information Security Education Pipeline

- There is a need for more information security workers
  - 56% of the US organizations indicated that they have too few number of information security workers ((ISC)², 2013)

- Not a diverse population of workforce and students
  - College of Information Sciences & Technology at the Pennsylvania State University
    - Percent of female students: 11% (26% in 1999)
    - Hispanic/Latino and African American students: 5%
Cyber Security Discovery Program Highlights

- A field trip to the Penn State Berks Campus (9:30am - 2:30pm)
- Max 20-24 students
- One session in each semester since 2010
- Hands-on learning in information security
Program Objectives

- Increase K-12 students’ interest in, and awareness about information security
- Introduce information technology/security career pathways
- Expose K-12 students to a college setting
- Have fun!
Participants

- Middle and high school students from the City of Reading
- Penn State Educational Partnership Program
Program

- **Morning Session: Computer Networking**
  - Computer networking (ipconfig, ping, tracert, sending messages, sharing folders)
  - User Accounts and File Permissions
  - Remote Access

- **Guest Speaker/Lunch Break (Questions and Answers)**

- **Afternoon Session: Cryptography**
  - Pencil Cipher, Caesar Cipher
  - Brute Force Attacks to Caesar Cipher
  - Code breaking with frequency analysis
  - Cryptography Games
Scytale (Stick) Cipher

- Students use a simple stick cipher to send secret messages to one another
- Learning Objectives & Conceptualization
  - Describe concepts such as algorithm, key, plaintext, and ciphertext
- Reflection & Active Experimentation
  - Identify the patterns how characters are shuffled
  - Different key

<table>
<thead>
<tr>
<th>Step 1. Preparation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2. Wrap the paper strip around the stick</td>
</tr>
<tr>
<td>Step 3. Type ATTACK AT DAWN vertically</td>
</tr>
<tr>
<td>Step 4. Unwrap the paper strip</td>
</tr>
</tbody>
</table>
Caesar Cipher

- **Learning Objectives**
  - Substitution ciphers
  - Key size

- **Reflection & Conceptualization**
  - How can Caesar Cipher be improved?

- **Active Experimentation**
  - Code breaking

(a) Caesar Cipher

(b) ROT13 Cipher

Crypto Club Caesar Cipher
Frequency Analysis and Code Breaking

- A code cracking competition activity
- The winning team explain their strategy and reasoning

Crypto Club Code Cracker
Cryptography Games

Desert Oasis Treasure Hunt

Clue #1 — Caesar Cipher — Key 3

Clear Plaintext

Choose a cipher tool that will help with this clue.
History & Synergy

2007 Wireless Summer Camp

- IST 220 Networking
- Estimating Wireless Coverage (4)
- $3500

2008 Northeast Pennsylvania Partnership for Workforce Development in Information Assurance (WIRED Grant)

- SRA 221 Security I
- Virtual Computer Lab (NPOL)
- Summer Camps (5)
- $45,000

2009 Leveraging Information Security Education and Training through Web-based Distance Learning

- IST 452 Security I
- IST 402 Ecommerce Security (online)
- Collaborative Virtual Computer Laboratory (CVCLAB)
- Discovery Days
- $55,000

2011 Exploration of a Collaborative Virtual Computer Laboratory (CVCLAB) to Enhance Distance Learning in Information Security (NSF DUE-No: 1044800)

- IST 452 Security I (online)
- Impact of Collaborative Work on Student Learning (>10)
- Hands-on Activities
- Discovery Days
- Undergraduate Research Assistants (>15)
- $155,000