EECS 388 Discussion 5

Review HW2, Web Practice

HW 2 Review - Part 1

- Substring analysis reveals 7 as a uniquely popular factor in lengths between repetitions
- Split into 7 distinct Ceasar ciphers corresponding to 7 positions in key
- Frequency analysis of these individual Caesar ciphers yield unique keys at each position: ENTROPY

HW 2 Review - Part 2c

- The variance decreases as the key length increases.
- You can think of this as the multiple copies of the English letter frequency distribution being offset from each other and averaged.

HW 2 Review - Part 2d

- Much closer to (b) than to (c).
- This is because the independent Caesar ciphers will have a frequency distribution similar to that of English text (and thus to that of the plaintext).

HW 2 Review - Part 2e

- The mean of the variances approximates the variance of the relative letter frequencies of English text when the assumed key size is correct.
- Can we find an alternative to the Kasiski Method?

Web Review

- SQL
  - injection attack
- HTML / Javascript (jQuery)
  - CSRF - Cross-Site Request Forgery
  - XSS - Cross Site Scripting

SQL Injection (Revisited)

- Consider a web server with route:

  `http://school.com/students?name=[name]`
- Runs this query on SQL database:

  `“SELECT * FROM STUDENTS WHERE NAME=” + name + “;”`
- How do we exploit this? What can we do to the database?

jQuery - Change HTML

```
<script>
$(function() {
    var url = "www.google.com";
    $("h3").html("<a target=\"run\" href=\"" + url + "\"> cool link! </a>");
});
</script>
<h3></h3>
```

- (function() { /*code to run on document ready*/ });
- $(“h3”).html(/* insert raw data as html at `h3` element */);

jQuery - Trigger Events

```
<script>
(function() {
    $("#testForm").submit();
});
</script>
<form name="myForm" id="testForm" method="POST" action="./userlogin">
UserName: <input type="text" name="user" value="test" /> <br/>
Password: <input type="password" name="password" value="test"/> <br/>
</form>
```

- submit a form element by id (using #)