

Final Assignment – due at the Final

CS 436/536/636

Option One: Encryption Paper

Write me a short paper (3-5 pages) about one of the following topics:

The Advanced Encryption Algorithm competition, who the finalists were, and why Rijndael became the new AES standard over the other finalists.

Choose one of the other AES finalists (not Rijndael/AES) and explain who wrote the algorithm, what their background was, and how the algorithm works.

DES is said to be crackable, and we know that it is. Choose one of the attack methods that are used to attack Block Ciphers, and explain how that type of attack is performed.

Option Two: SQL Injection

Attempt an SQL Injection attack against one of the vulnerable online banking test systems shared in Monday's lecture.

Explain what techniques you try and what the results are.

Explain what the underlying data structure is, and how you can tell.

For bonus credit, provide the userids and passwords that you retrieve via web-SQL injection.

ONLY USE THESE THREE WEBSITES. DO NOT USE THESE METHODS ANYWHERE ELSE!!!!

- <http://zero.webappsecurity.com/>
- <http://testphp.acunetix.com/>
- <http://demo.testfire.net/>