Cryptography Report: Analysis of Cryptographic Tools (Date assigned: April 1, 2019)

OVERVIEW: This is an individual report identifying a cryptographic tool or process that should be retired and the new tool or process that should replace it.

DETAILS:

Each student will be required to write a research paper identifying an existing cryptosystem with deficiencies and proposing a replacement cryptosystem that improves cryptographic security for the intended function. The paper must cover
*the weakness(es) of the existing system
*how the replacement system mitigates the weakness(es), and
*if weaknesses remain or are introduced by the replacement system, there must be a justification of the benefit of replacing one vulnerable cryptosystem with a different vulnerable cryptosystem.
*The criteria for the assignment is that the existing system must have one or more known vulnerabilities, and the replacement system must be accepted as generally more secure against attacks than the identified vulnerable system.

The target audience for this paper is the IT and security and risk departments of a commercial or governmental organization. Your role is to be the security analyst attempting to improve the security of the organization. Your paper will become part of an organizational review to determine if operational policies and practices should be updated. Please write addressing a business audience, not an academic audience.

The paper should be no more than 8 pages in length (double-spaced, 10 to 12 point type, with standard margins). Papers shorter than 8 pages which fully cover the report requirements will not be penalized. In business, making your case without being lengthy is rewarded. At the same time, you must provide credible evidence to support your recommendations. Citations and bibliographic references, if you choose to use them, are not considered in the page count. No more than 50% of the document can be relevant diagrams or other graphics.

EXAMPLE:
1. Why WEP is bad
2. How WPA2 resolves the WEP crypto weaknesses
3. How to employ WPA2 securely (minimum key length; don't use WPA2/PSK, etc.)

Candidate topics

MD5 Hash
HTTPS using SSL
NTLM Windows authentication system
Single-factor Authentication
One-way authentication (as opposed to mutual authentication)
Windows local authentication
Unix/Linus local authentication

As the author, you are free to choose any two related cryptosystems for your report, but you will be graded on whether the systems meet the report requirements.

The paper is due not later than April 13

This paper will be 20% of the total course grade.