

Cybersecurity Guided Notes

Lesson 2.8.1 - Hashing and Digital Signatures

1. Explain the difference between cryptography and cryptanalysis.

2. Match the following term with their definition.

- | | |
|-------------------|--|
| A. Ciphertext | _____ A one-way encryption that converts any form of data into a unique string of text known as a digest |
| B. Plaintext | _____ The message that has been encrypted that typically looks like jumbled mess |
| C. Key Stretching | _____ The addition of text to a password before hashing it and then storing the value with the hash |
| D. Hash | _____ Used to convert a password to a longer and more random one |
| E. Collision | _____ The message to be sent which has not been encrypted yet |
| F. Salting | _____ When you have two different inputs that produce the same hash |

3. What happens if your private key is made public?

4. What should occur if a hash algorithm is found to have collisions?
5. What are the three most common applications for hashing?
6. How are passwords stored/verified and why is it stored this way?
7. What proof does digital signatures provide?