Cryptography Terminology

Tom Kelliher, CS 400

Cryptography is used to maintain:

- Message secrecy/privacy: Foreign parties can't read the message.
- Message integrity: Foreign parties can't manipulate the message.
- Message authenticity: The receiver has assurance that the sender is who they claim to be.

Terminology lookup terms:

1. Forward and Backward Secrecy: What are they? (Gabe)
2. Message Authentication Code: What is it used for? (Gabe)
3. Digital Signature: How is a signature and the signed "document" verified? (John)
4. Diffie-Hellman Key Exchange: How do the two parties construct the shared session key and how do they exchange it and keep it private? (John)
5. Key Updating and Autokeying: What are they? Why are they useful? (Tom)