1. The Secure Hash Algorithm (SHA) was developed by the NIST and published as a federal information processing standard (FIPS 180) in 1993.

2. Versions of SHA, with hash value lengths of 256, 384, and 512 bits, (SHA-256, SHA-384, and SHA 512) are collectively known as SHA-2.

3. The evaluation criteria for the new hash function are: security, cost and algorithm and implementation characteristics.

4. HMAC has been issued as RFC 2014, has been chosen as the mandatory-toimplement MAC for IP Security, and is used in other Internet protocols, such as Transport Layer Security.

5. One of the first public-key schemes, RSA was developed in 1977 by Ron Rivest, Adi Shamir, and Len Adleman.

6. Timing attacks are alarming for two reasons: they come from a completely unexpected direction and they are a ciphertext-only attack.

7. Four possible approaches to attacking the RSA algorithm are: brute force, timing attacks, mathematical attacks, and chosen ciphertext attacks.

8. NIST has published FIPS PUB 186, which is known as the DSS.

9. The purpose of the secret key algorithm is to enable two users to exchange a secret key securely that can then be used for subsequent encryption of messages.

10. One of the simplest hash functions is the XOR of every block.

11. “Must support hash value lengths of 224, 256,384, and 512 bits” and “algorithm must process small blocks at a time instead of requiring the entire message to be buffered in memory before processing it” are requirements for SHA-3.  
12. If speed is a concern, it is fully acceptable to use MD5 rather than SHA as the embedded hash function for HMAC.

14. The security of any MAC function based on an embedded hash function depends in some way on the cryptographic strength of the underlying hash function.

15. Perhaps the most widely used public-key algorithms are RSA and DiffieHellman.