

COMP3260/COMP6360 Data Security Week 10 Workshop – 16th and 17th May 2019

1. Alice and Bob use the Diffie-Hellman key exchange technique with a common prime $q = 157$ and a primitive root $\alpha = 5$.
 - a. If Alice has a private key $XA = 15$, find her public key YA .
 - b. If Bob has a private key $XB = 27$, find the public key YB .
 - c. What is the shared secret key between Alice and Bob?

2. Solve the following problem, now as Birthday Paradox, and use the solution to analyse the Birthday Attack on a hash function.

Birthday Paradox: What is the minimum value of k such that the probability is greater than 0.5 that at least two people in a group of k people have the same birthday?

3. Prove that in DSA signature verification we have $v = r$ if the signature is valid.

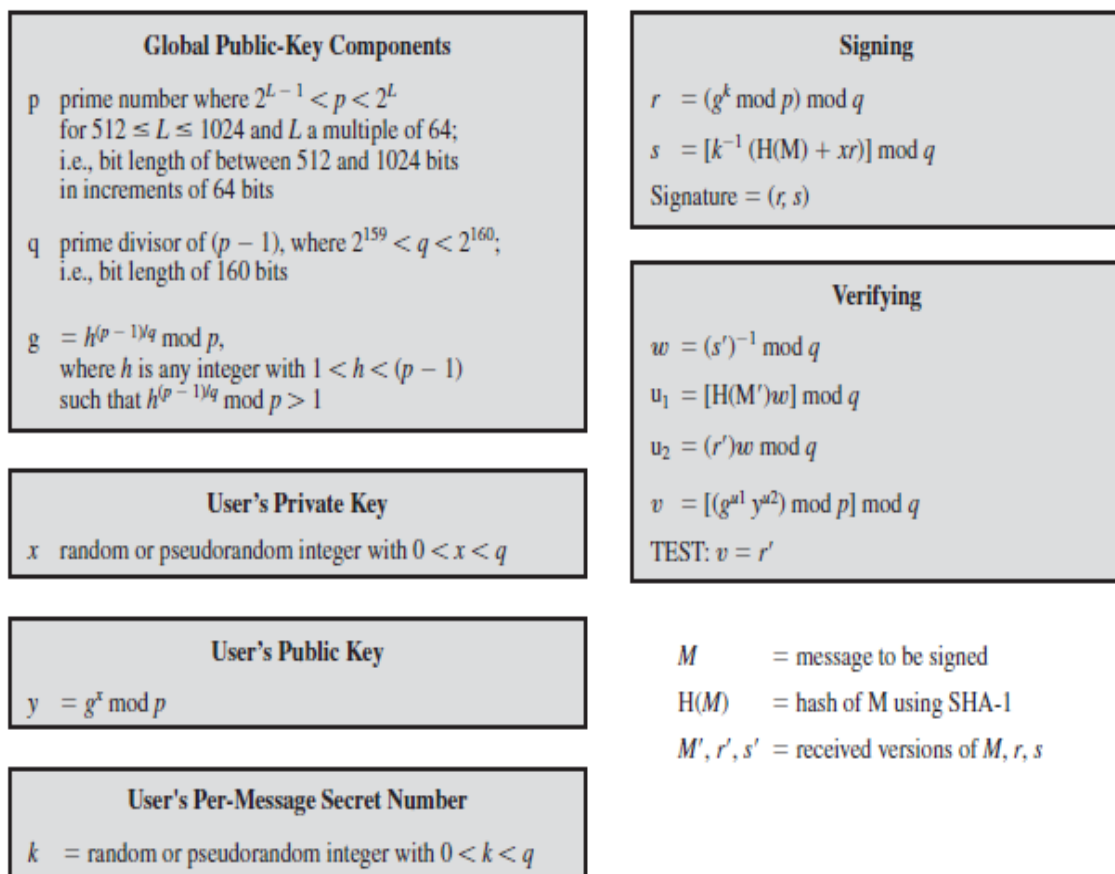


Figure 13.4 The Digital Signature Algorithm (DSA)