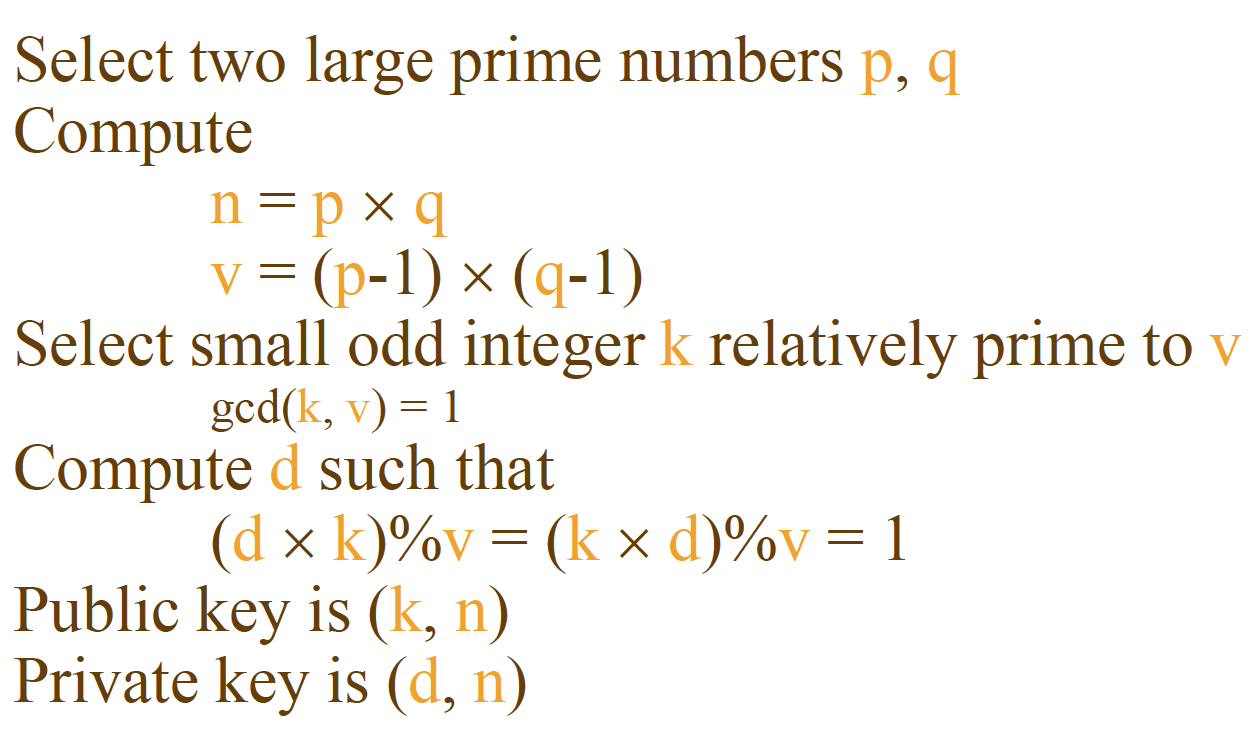


1. Active attack such as falsification of data and transactions. This can include falsifying the source or damaging the integrity of the data by unauthorized modification.
2. RSA Attacks - Attack RSA that may be used in encryption. This can be done with a brute force attack attempting to exhaust the key space.
   1. Mathematical attacks to determine key
      1. RSA - Determine n by factoring n = p \* q. Using this as a means to compute d (d can also be found directly). Please refer to algorithm below.



* 1. Timing attacks
     1. Trying to use the decryption time to discover the key.
  2. Hardware fault attacks – can be in the hardware or software. Faults may cause errors and these errors can be leveraged for information. Faults can be introduced to increase the chances of an error occurring.

1. Created by NIST to go over all applications of encryption for using block ciphers. Block ciphers turns plain text into a fixed number of blocks equal in size containing cipher text. Modes of operation were designed to encipher text of any size using any symmetric block cipher such as Data Encryption Standard (DES) and Advanced Encryption Standard (AES). DES and AES are symmetric block ciphers. Symmetric refers to a single key for encryption and decryption of plain and cipher text. The opposite is Asymmetric cryptography, which involves two keys – a public and private key.
2. Applications
   1. Digital Signature – A digital signature is an electronic document that verifies an author, date and time of signature. An example would be an e-signature to verify the identity of the sender and to confirm the integrity of a document. A digital signature creates a hash from a private key and signature. Verifying a digital signature referencing the original message and public key.
   2. Digital Certificate – A digital certificate verifies ownership of a public key. The Certification Authority (CA) creates trusted certificates and has a public key that is built into web browsers. A CA issues a certificate by forming a signature on the public key and identity of its owner.
   3. Examples of uses of Asymmetric key use
      1. Digital Signature Standard – Creates digital signature using SHA-1
      2. Elliptic-Curve Cryptography (ECC) – Complex, small key size, but provides security. There is low confidence level in ECC due to being around for a few years while algorithms like RSA have been around for 30 years.[[1]](#footnote-1)
      3. Diffie-Hellman – Algorithm to exchange a secret key securely – it is difficult to computer discrete logarithms.
      4. RSA – Uses prime numbers in its secret key. It is assumed to be difficult to factor integers into their prime numbers.

Differential cryptanalysis is used to break cryptosystems. A cryptosystem is an algorithm that takes a key and converts plain text into cipher text. Analyzing the difference between two inputs and observing its characteristics may lead to cracking a key. The difference between the two inputs is a XOR function. The goal of differential cryptanalysis is to find a key through lesser work. For example an exhaustive approach would be to brute force the key space. Cryptanalysis can reduce the time to find a key. Cryptanalysis can vet an algorithm’s strength. For example, SHA-2 and SHA-3 may be susceptible to unknown attacks, but cryptanalysis as reassured confidence that the algorithm is strong.

<http://cs.ucsb.edu/~koc/ccs130h/notes/dc1.pdf>

<https://www.cs.columbia.edu/~smb/classes/f06/l03.pdf>

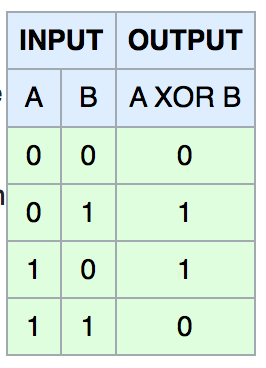
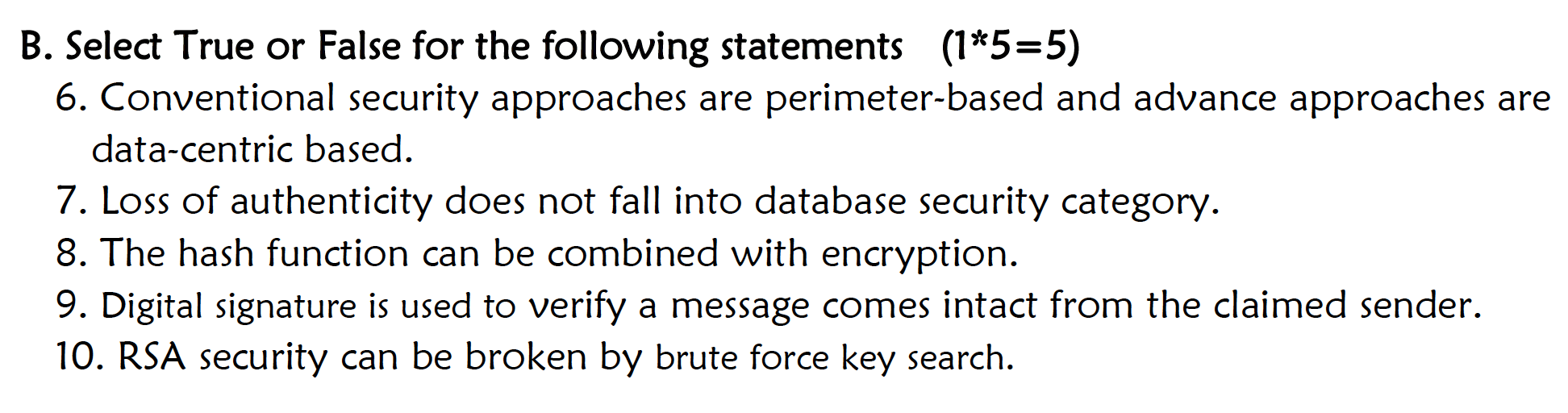


Figure - XOR Gate

<https://en.wikipedia.org/wiki/XOR_gate>



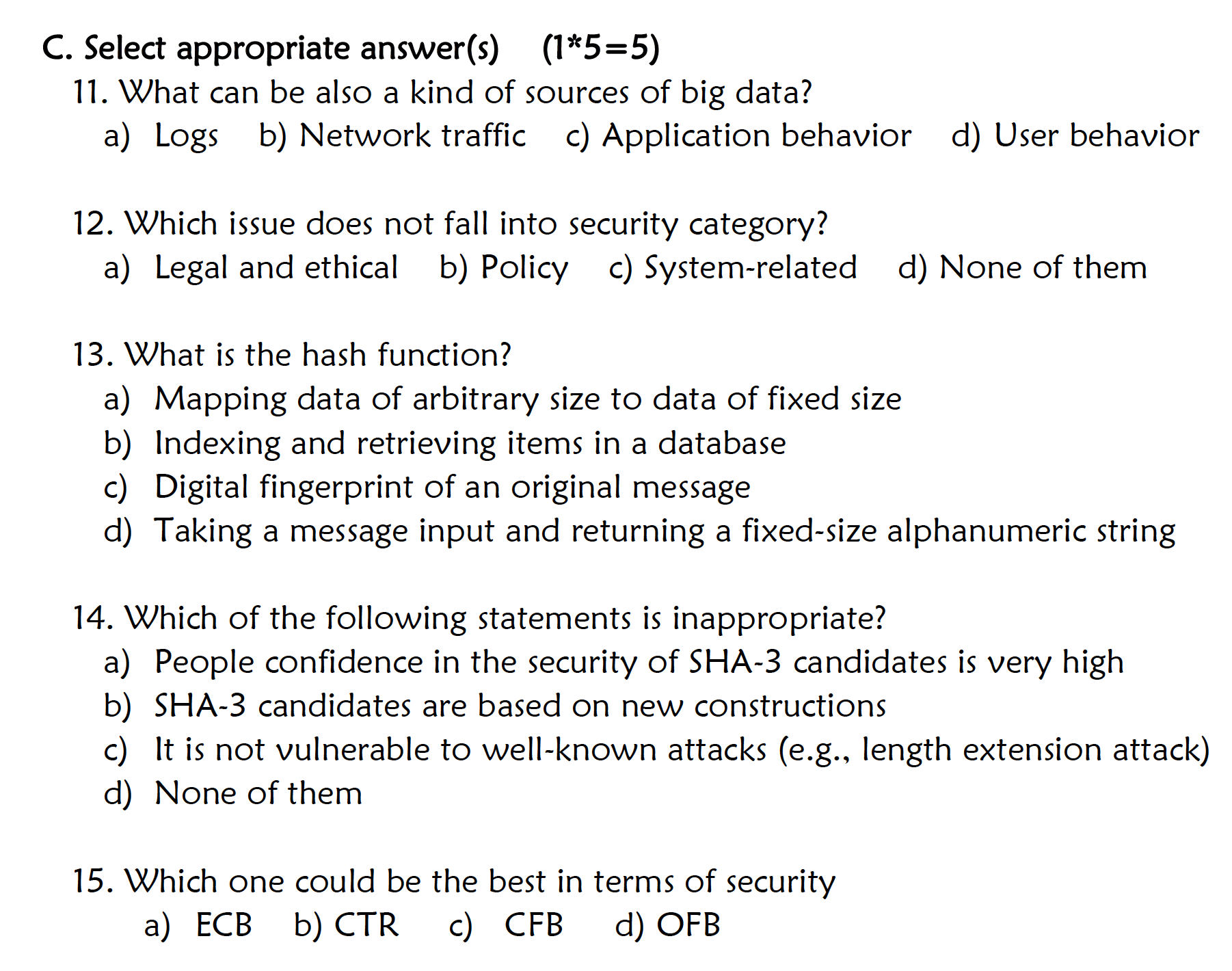
?

false

true

true

true



A,B,C,D

D

C

C

B

1. Taken from Lecture 3 slides [↑](#footnote-ref-1)