CSc 4222/6222 Assignment 5
Hard copy due: Dec. 3, 12:30pm

1. Describe a method for protecting users against URL obfuscation attacks.

2. Suppose a web client and web server for a popular shopping web site have performed a key exchange so that they are now sharing a secret session key. Describe a secure method for the web client to then navigate around various pages of the shopping site, optionally placing things into a shopping cart. Your solution is allowed to use one-way hash functions and pseudo-random number generators, but it cannot use HTTPS, so it does not need to achieve confidentiality. In any case, your solution should be resistant to HTTP session hijacking even from someone who can sniff all the packets.

3. What is the encryption of the following string using the Caesar cipher: INFORMATIONSECURITY?

4. Compute the multiplicative inverse of 7 in Z23.

5. Show the steps and intermediate results of applying the extended Euclidean algorithm to compute the GCD of 512 and 240.

6. Find keys d and e for the RSA cryptosystem with p = 17 and q = 11; encrypt a given message M=88; show your steps. (Tips: you may use the following site is helpful in calculation: https://www.wolframalpha.com/input/?i=19%5E5+mod+119)

7. Demonstrate that the hash function H(x) = 5x + 11 mod 19 is not weakly collision resistant, for H(4).

8. Explain why nonforgeability and nonmutability imply nonrepudiation for digital signatures.

9. Alice wants to send a large document as an encrypted attachment to an email to Bob over the internet. Alice also wants Bob to know that this attachment was sent by her (and not a forged attachment sent by someone else). Assume Alice and Bob have each other's public keys.
   In the questions below, use the cryptographic primitives we've discussed in class. Define any cryptographic functions that you use. For example: one could say:
   - H is cryptographic hash function, or H is MD5;
   - PKa, SKa, PKb, SKb - Alice and Bob's public/private key pairs
   - Ek()/Dk() -- Authenticated encryption/decryption scheme using key k (say, AES-GCM)

- Enc()/Dec() -- Public key encryption/Decryption (say, RSA encryption)
- Sign/Verify -- Digital signature/verification algorithm (say, RSA signature)

A. Give the steps for Alice to prepare the attachment that will be sent.

B. Give the steps for Bob to decrypt Alice's attachment and verify that the message is valid and authentic (it has not been tampered and it was definitely sent by Alice).

10. Bitcoin transactions cannot be reversed. Explain why, referencing its technical design features as needed.