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

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

Solution This method requires modi_cations to the browser. Expand non-ASCII Unicode characters into strings so that they cannot be confused with similar ASCII characters. Also, highlight as potentially dangerous any hyperlinks whose target is different from the URL displayed and require user confirmation before following them.

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.

Solution Seed the PRNG with the secret key and include in each HTTP request the next pseudo-random number in the sequence, as well as a userID, as a part of the URL. The server can determine that this is the specified user, because even an eavesdropper would not be able to determine the next number in the PRNG.

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

Note: student can specify any # as the key to shift or substitute. The following is just one example answer.

Plain text: INFORMATION SECURITY

Caesar cipher table:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W

Ciphertext : F K C L O J X Q F L K P B Z R O F Q V

4. Compute the multiplicative inverse of 7 in Z23.

Because 7 and 23 are relative primes, 7 has its multiplicative inverse.

23 =7*3 + 2 *and* 7 = 3*2+1
So 1 = 7 − 3*2 = 7 − 3*(23 − 7*3) = 7(10) − 23(3) From 23(3) + 1 = 7(10) ,
the multiplicative inverse of 7 is 10.

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

Gcd(512,240) = gcd(240, 512 mod 240) =>gcd(240, 32)
=gcd (32, 240 mod 32) =>gcd(32,16)
=gcd(16,32 mod 16) =>gcd(16,0)
gcd(512,240) = 16
Therefore, the gcd of 512 and 240 is 16.

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)

1. Select primes: p=17 & q=11
2. Compute $n = pq$ =17×11=187
3. Compute ø(n)=(p–1)(q-1)=16×10=160
4. Select e *:* gcd(e,160)=1; choose e=7
5. Determine d*:* de=1 mod 160 and d < 160 Value is d=23 since 23×7=161= 10×160+1
6. Publish public key KU={7,187}
7. Keep secret private key KR={23,17,11}
8. given message M = 88 (nb. 88<187)
9. encryption:
10. C = 88^7 mod 187 = 11

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

H(x) = (5x + 11) mod 19
H(4) = (20+11) mod 19 = 12
19y+12-11 = 5x => 19y+1 = 5x, 19y+1 has to be multiples of 5
Search for 19y value where 19y+1 mod 5 = 0
19*6=114, 114+1/5 = 23
19*11=209 209+1/5 = 42
19*16=304 304+1/5= 61
19*21=399 399+1/5 = 80

H(23),H(42),H(61),H(80) all has same hashed value, the hash function is not weakly collision resistant.

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

Solution The reason non-forgeability and non-mutability imply non-repudiation is that a signature, SAlice(M), produced by Alice, is easily veri_able using publicly available infor-
mation, and it is computationally infeasible for an attacker to have forged this signature from scratch or to have transformed a di_erent signature into this one (and have it still be veri_able for the message M). So Alice must have been the one to produce this signature and the message M must have been what she was signing when she did this.

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.
// Choose random, one-time symmetric key, then encrypt the attachment M
k = rand_key()
C1 = Ek(M)
// Encrypt k with Bob's public keyand sign the entire ciphertext with Alice's private key
C2 = Enc(PKb, k)
sig = Sign(SKa; C1,C2)
Send: C1,C2,sig

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).
// Verify the digital signature using Alice's public key
if Verify(PKa; sig; C1,C2) = INVALID: return ERROR
// Decrypt the symmetric key with Bob's private key, then decrypt the attachment

k’ = Dec(SKb, C2)
M’ = Dk’(C1)
if M’ = ERROR: return ERROR
else: return M’

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