Review for Exam 2: Breakout Puzzles

Puzzle 1: Number Base Conversions

1) Convert 92,853 from decimal to hexadecimal.
2) Convert 202 from decimal to binary.
3) Convert 2981 from decimal to octal.
4) Convert 157 from decimal to binary.

Puzzle 2: Encryption

1) Alice wants to send Bob a secret message using asymmetric key encryption. What does she need from Bob in order to do so?
2) Alice wants to make sure that she has Bob's public key, and not the public key of an imposter. What can she use to verify the authenticity of Bob's public key?
3) Alice uses Bob's public key to send him a shared secret, "blockchain7". Use this public key and tinyurl.com/satoshisymmetric to encrypt a secret message, "protect satoshi's bitcoin". Write the first six characters of the ciphertext below:
4) What can Bob use to verify that Alice is the only person who could have possibly sent this message?

Puzzle 3: Bits & bytes

1) Suppose you are using an encryption protocol that uses 5l2-bit keys. If you wanted to adopt a new protocol that would take l6 times longer for a purely brute-force attack, how many additional bits should be added to the keys?
2) How many binary bits are needed to store a single extended (padded) ASCII character?
3) How many binary bits are required to store the value of a Boolean variable?
4) What is the value of "a" after running the following algorithm?

```
a ← 6
b ← a/3
a ← a*b
b ← a – b
a ← b
a ← a/2
```

Puzzle 4: Programming

Station 1, Part A:

```
var list = [0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12];
function mystery(inputArray) {
        var output = 0;
        for (i = 0; i < inputArray.length; i++){
                if (inputArray[i] % 3 == 0){
                        output++
                }
        }
        return output
}
var answer1 = mystery(list);
```

Station 1, Part B:

Which of the following Describes the length of time a packet of data takes to get from client to server?
5) bitrate
6) bandwidth
7) latency
8) cache

answer2 = _____

Station 1, Part C:

convertToHex(answer1 + answer2)

Station 2, Part A:

Which of the following inequalities is always true?

l) bitrate < bandwidth
m) bitrate > bandwidth
n) bitrate <= bandwidth
o) bitrate >= bandwidth
p) not enough information to determine.

answer1 = _____

Station 2, Part B:

```
var steps = 0;
var total = 0;
while (steps < 5 && total < 15){
        steps++;
        total += steps + total;         // notice that this is a +=
}
var answer2 = total – 15;
```

Station 2, Part C

caesar(answer1, answer2)

Station 3, Part A

Which of the following is true?

1) The DNS protocol allows a web browser to find an IP address from a URL.
2) The TCP protocol breaks data down into packets for transmission (or reassembles them upon receipt).
3) The IP protocol puts appropriate "To" and "From" addresses onto packets.
4) The TCP/IP protocols do not encrypt data, but TLS/SSL can be used to encrypt HTTP requests. This is the basis of the HTTPS protocol.
5) All of the above.

answer1 = _____

Station 3, Part B

x ← 5
y ← 2*x
y ← x + y
y ← y/3
x ← 1

answer2 ←x + y

Station 3, Part C

convertToHex(answer1 + answer2)

Station 4, Part A:

When a web browser tries to access a website such as www.w3schools.com, In what order are the following protocols invoked?

A) DNS

E) IP

T) TCP

Station 4, Part B:

‘aet’ = D
‘ate’ = E
‘eat’ = F
‘eta’ = G
‘tae’ = H
‘tea’ = I

Station 5, Part A:

```
var list = [0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15];
function mystery(inputArray) {
	var outputArray = [];
	for (i = 0; i < list.length; i++){
		var item = inputArray[i];

		if (item % 5 == 0){
			outputArray.push(item);
		}
	}
	return outputArray;
}

var myArray = mystery(list);
var key = myArray[3];
```

Station 5, Part B:

caesar(‘c’, key)

Puzzle 5: Data

1) All of the following are ways that a research team can try to protect an individual's privacy. Which is most likely to be effective?

   (C) Store data on a webserver, and only grant server access to authorized employees.

   (B) Outsource cloud data storage to a company specializing in secure data storage solutions.

   (S) Regularly update software and apply security patches on servers containing sensitive data.

   (T) Obfuscate the data so that it cannot be linked to any single individual.

2) Which of the following is best describes a benefit of cloud computing?

   (R) Cloud computing is less susceptible to a data breach than storing files locally.

   (L) Cloud computing reduces the chance that advertisers and data brokers will access an individual's sensitive data.

   (H) Cloud computing allows individuals to access their data in more locations and on more devices.

   (E) Individuals get more control about how their data is used and stored compared to storing files locally.

3) Which of the following will affect the ability of a program to process a large data set?

   (O) The amount of additional processing power the program requires per additional entry in the data set.

   (I) The amount of additional memory (RAM) the program requires per additional entry in the data set.

   (E) The amount of additional hard drive space the program requires per additional entry in the data set.

   (A) All of the above.

4) Which of the following is least likely to be partly attributable to Moore's Law?

(T) The need for longer encryption keys over time.

(D) The increasing ability of data scientists to process large data sets.

(W) The creation of the open Internet protocols such as DNS, TCP/IP, HTTP, and TLS/SSL.

(P) Advances in machine learning and artificial intelligence, such as Google’s AlphaGo.

Puzzle 1: Answers

1) 16AB5
2) 11001010
3) 5645
4) 10011101

Puzzle 2: Answers

1) Public key
2) Digital certificate
3) 8fca2d
4) Digital signature

Puzzle 3: Answers

1) 4
2) 8
3) 1
4) 5

Puzzle 4: Answers

Station 1, Part A: 5
Station 1, Part B: 7
Station 1, Part C: convertToHex(5 + 7) = convertToHex(12) = C

Station 2, Part A: N
Station 2, Part B:11
Station 2, Part C: caesar(N, 11) = Y

Station 3, Part A:
Station 3, Part B: 5
Station 3, Part C: convertToHex(11) = B

Station 4, Part A: “ATE”
Station 4, Part B: “ATE” = E

Station 5, Part A: 15
Station 5, Part B: caesar(‘C’, 15) = R

Overall puzzle: CYBER

Puzzle 5: Answers

1) T
2) H
3) A
4) W