Encoding (Base64)

Which statements about Base64 encoding are correct?

- □ a. Base64 adds a layer of security.
- ☑ b. Base64 translates binary data to ASCII printable characters.
- □ c. Base64 is necessary to send binary data over TCP channels.
- ☑ d. Base64 encoded channels exhibit higher network traffic.

Which statements about Base64 encoding are correct?

- □ a. Base64 is a hash-based encoding scheme.
- □ b. Base64 encoded messages are less vulnerable to man-in-the-middle attacks.
- ☑ c. Encoding messages with Base64 increases their data size.
- ☑ d. Base64 encoding is necessary to send binary data over plain text channels.

What are the benefits of using Base64 encoding?

- □ a. The security is enhanced as the data is additionally encrypted with Base64.
- ☑ b. It is possible to transmit any kind of data as a text string.
- □ c. The data throughput is increased because of the higher bit-rate of Base64.
- ☑ d. Control characters are converted to printable ASCII characters.

Hashing

Message integrity means that the data of a message ...

- ☑ a. ... is not corrupted in transit.
- □ b. ... is encrypted.
- □ c. ... is not read by a third party.
- ☑ d. ... is not tampered with by a third party.

HMAC

To generate a Hash-based message authentication code (HMAC) one needs:

- ☑ a. A shared secret key.
- □ b. A public and private key.
- □ c. Only an appropriate hash function.

Hash-based message authentication codes (HMAC) are used to:

- ☑ a. verify the source of a message.
- □ b. verify that a message cannot be read by a third party.
- ☑ c. verify the integrity of a message.

What distinguishes a MAC (Message Authentication Code) from an ordinary Hash function?

- □ a. By using a MAC a message gets encrypted before being hashed.
- ☑ b. By using a MAC a message and a secret key get hashed to ensure message integrity.
- □ c. When applying an ordinary hash function to a message, that message can not be reconstructed from the corresponding hash, while this is possible when applying a MAC to a message.
- □ d. Hashes generated by a MAC function are much smaller in size than hashes generated by ordinary hash functions and are therefore better suited for network transfer.

Which statement(s) hold true for Message Authentication Codes (MAC):

- □ a. A message is encrypted with a shared key before sending and the resulting ciphertext is transferred alongside with the original message.
- □ b. A message is encrypted and hashed before sending and the resulting hash is transferred alongside with the original message.
- ☑ c. A message and a shared secret are hashed before sending and the resulting hash is transferred alongside with the original message.
- □ d. A message and the public key of the authenticated receiver are hashed before sending and the resulting hash is transferred alongside with the original message.

Cryptography

Which statement(s) hold true regarding cryptography:

- □ a. Asymmetric cryptography is significantly faster than symmetric cryptography.
- □ b. If possible, asymmetric cryptography should always be preferred over symmetric cryptography.
- ☑ c. Asymmetric cryptography can be either used for encryption or signing.
- ☑ d. The exchange of a common key bears a potential risk for symmetric cryptography.

Which statement(s) regarding security hold true:

- ☑ a. Data integrity refers to the fact that data must be reliable and accurate over its entire lifecycle.
- ☑ b. Data encryption is a common method of ensuring confidentiality.
- □ c. Data encryption is a common method of ensuring integrity.
- ☑ d. Confidentiality concerns with protecting sensitive information from disclosure to unauthorized parties.

Asymmetric cryptography

Asymmetric cryptography: To make sure only the intended receiver can decrypt a message, it has to be encrypted with the receiver's public key.

- ☑ Wahr
- □ Falsch

Asymmetric cryptography: To make sure only the intended receiver can decrypt a message, it has to be encrypted with the sender's private key.

□ Wahr
☑ Falsch

Asymmetric cryptography: The only way to encrypt a message is to use the public key, while the private key can only be used for decryption.

□ Wahr
☑ Falsch

In asymmetric cryptography, which key is used to encrypt a message?

□ a. The sender's private key.
□ b. The receiver's private key.
□ c. The sender's public key.
☑ d. The receiver's public key.
□ e. The shared secret key.

In asymmetric cryptography, which key is used to decrypt a message?

□ a. The sender's private key.
☑ b. The receiver's private key.
□ c. The sender's public key.
□ d. The receiver's public key.
□ e. The shared secret key.

RSA is an example of a symmetric encryption protocol.

□ Wahr
☑ Falsch

Symmetric cryptography

In symmetric cryptography, which key is used to encrypt a message?

□ a. The sender's private key.
□ b. The receiver's private key.
□ c. The sender's public key.
□ d. The receiver's public key.
☑ e. The shared secret key.

In symmetric cryptography, which key is used to decrypt a message?

□ a. The sender's private key.
□ b. The receiver's private key.

- □ c. The sender's public key.
- □ d. The receiver's public key.
- ☑ e. The shared secret key.

Which statements about symmetric key encryption are correct?

- □ a. RSA is an example of symmetric encryption.
- ☑ b. AES is an example of symmetric encryption.
- ☑ c. The same key is used for encryption and decryption.

Symmetric encryption techniques make use of key pairs (public and private key) to encrypt and decrypt messages.

- □ Wahr
- ☑ Falsch

TCP

The three way handshake is used for establishing a TCP connection.

- ☑ Wahr
- □ Falsch

What type of service does TCP provide? Tick all that apply.

- ☑ a. reliable
- □ b. unreliable
- ☑ c. connection-oriented
- □ d. connection-less

Which statements about TCP are correct?

- ☑ a. TCP automatically re-transmits lost packages.
- □ b. TCP is a connectionless protocol.
- ☑ c. TCP guarantees that packets are received in the order they were sent.
- □ d. TCP is useful when the loss of individual packets is unimportant.

Which procedure is used to establish a TCP connection?

- □ a. Request/response messaging
- □ b. Two-way handshake
- ☑ c. Three-way handshake
- □ d. TCP does not require connection establishment

UDP

If two hosts are communicating via UDP, both sides have to use the same port number for the UDP communication.

- □ Wahr
- ☑ Falsch

Which procedure is used to establish a UDP connection?

- □ a. Request/response messaging
- □ b. Two-way handshake
- □ c. Three-way handshake
- ☑ d. UDP does not require connection establishment

Which statements about UDP are correct?

- □ a. UDP re-transmits lost packages.
- ☑ b. UDP is a connectionless protocol.
- □ c. UDP guarantees that packets are received in the order they were sent.
- ☑ d. UDP is useful when the loss of individual packets is unimportant.

Which statements about UDP are correct?

- □ a. It is the object-oriented equivalent of remote procedure call (RPC).
- □ b. It relies on the publish/subscribe messaging pattern.
- □ c. It simplifies the coordination of multi-threaded programs.
- □ d. It simplifies data exchange between Java programs.

Sockets

In order to establish a connection with a server socket, is it required to manually specify the local port number of the Java client socket?

- □ a. Yes, the local port has to be specified upon creation of the client socket.
- ☑ b. No, the underlying platform will choose a free port at random.
- □ c. No, the client socket will automatically negotiate a port number with the server socket via the handshake protocol.

Mark the correct answers concerning TCP and UDP Sockets in Java:

- ☑ Wahr
- □ Falsch

Consider the following code that reads from a network socket:

```
BufferedReader reader = new BufferedReader(...);
```

```
while (!Thread.interrupted()) {
  String line = reader.readLine();
  System.out.println(line);
}
```

Suppose the underlying socket is waiting on new data, but the executing thread is interrupted using `Thread.interrupt()`, what happens?

- ☐ a. *null* is printed on `System.out` and then the loop terminates.
- ☑ b. Nothing, `readLine()` continues to block.
- ☐ c. An `InterruptedException` is thrown and the method exits.

What happens when the `close()` method of a `ServerSocket` is called?

- ☐ a. All socket connections that were accepted by the `ServerSocket` are closed.
- ☑ b. The `ServerSocket` stops listening to new connection requests.
- ☐ c. The connected clients receive an exception that the `ServerSocket` was closed.

Similar to `java.net.Socket`, the input/output streams of `java.net.DatagramSocket` have to be closed.

- ☐ Wahr
- ☑ Falsch

Which types of connections does `java.net.ServerSocket` accept?

- ☐ a. UDP connections.
- ☑ b. TCP connections.
- ☐ c. TCP and UDP connections.

Consider the following code that reads from a network socket:

```
BufferedReader reader = new BufferedReader(...);
try {
  String line = reader.readLine();
  System.out.println(line);
} catch(InterruptedException e) {
  System.out.println("interrupted");
}
```

Suppose the underlying socket is waiting on new data, but the executing thread is interrupted using `Thread.interrupt()`, what happens?

- ☑ a. Nothing, `readLine()` continues to block.
- ☐ b. *null* is printed to `System.out` and the method exits.
- ☐ c. *interrupted* is printed to System.out and the method exits.

To establish a bidirectional communication between a server and a client through Java sockets, how many sockets and streams do you need at least on each side?

☑ a. 1 socket, 1 output stream and 1 input stream on each side (2 sockets, 4 streams in total on both sides).
☐ b. 2 sockets per side, each with 1 output stream and 1 input stream (4 sockets, 8 streams in total on both sides).
☐ c. 1 socket with 1 output stream plus 1 socket with 1 input stream, on each side (4 sockets, 4 streams in total on both sides).

DMAP & DMTP (handshake and startsecure)

Which statements about the *startsecure* handshake protocol implemented in Lab 2 are correct?

☑ a. Its purpose is to be guard against replay attacks (a once valid transmission is fraudulently repeated or delayed).
☑ b. During the handshake, the sender uses the receiver's public key for encryption.
☐ c. The initial handshake (encrypted via AES) is used to safely exchange the RSA key.
☐ d. After the handshake, the data transferred over the network changes from plain text to binary.

What is true about the challenge-response authentication protocol (as used in the Lab):

☑ a. Its purpose is to be safe against replay attacks (a once valid transmission is fraudulently repeated or delayed).
☐ b. During the handshake, the sender uses the receiver's private key for encryption.
☑ c. The initial handshake (encrypted via RSA) is used to safely exchange the AES keys

What are valid ways to implement mail forwarding in the TransferServer according to the DSLab assignment? Suppose

☑ a. Make DMTP connection handlers write mails into `a java.util.concurrent.BlockingQueue`, and use a worker thread to continuously reads and forward mails from that queue.
☑ b. Use an Executor returned by `Executors.newFixedThreadPool`, and let DMTP connection handlers submit new 'MailForwarder' threads using the executor.
☐ c. Use an Executor returned by `Executors.newCachedThreadPool`, and let DMTP connection handlers submit new 'MailForwarder' threads using the executor.
☐ d. Let DMTP connection handlers spawn a new 'MailForwarder' thread after each message is received.

Which properties does the DMAP (DSLab Message Access Protocol) protocol have?

☐ a. Stateless
☑ b. Plain-text
☑ c. Stateful

☐ d. Binary

Which properties does the DMTP (DSLab Message Transfer Protocol) protocol have?

☐ a. Binary
☑ b. Plain-text
☐ c. Asynchronous
☑ d. Synchronous

Which statements about the *startsecure* handshake protocol implemented in Lab 2 are correct?

☑ a. Its purpose is to be guard against replay attacks (a once valid transmission is fraudulently repeated or delayed).
☐ b. During the handshake, the sender uses the receiver's private key for encryption.
☑ c. The initial handshake (encrypted via RSA) is used to safely exchange the AES key.

Java synchronization

When a synchronized method is called in Java, a lock is obtained on:

☑ a. The object (this)
☐ b. The method
☐ c. The class
☐ d. The variables used in the method

If a method with the signature `synchronized void doWork() {...}` is accessed by two different threads on the same object instance, only one of the threads can execute at a time.

☑ Wahr
☐ Falsch

Mark the correct answer(s) concerning concurrency and synchronization in Java:

☐ a. If a `java.util.HashMap` is accessed only by retrieving it from a getter method, the `HashMap` can be made thread-safe by writing the `synchronized` keyword in front of that getter method.
☑ b. A `java.util.HashMap` may throw a `ConcurrentModificationException` even with perfectly proper synchronization.
☐ c. If a class is defined as synchronized (e.g., `public synchronized class Foo`) then all methods of this class are automatically thread safe.
☑ d. Adding the `synchronized` modifier to the method signature is effectively equivalent to enclosing the body of the method with a `synchronized(this) {...}` block.

At which layer of the OSI model does the DMTP (DSLab Message Transfer Protocol) protocol operate?

☑ a. L7: Application Layer
□ b. L4: Transport Layer
□ c. L3: Network Layer
□ d. L2: Data Link Layer

Java threading

Imagine you want to execute Java code in a new Thread. One possibility is to write a class `MyExecutable` that implements the interface `java.lang.Executable` and to create a new Thread that executes the code in `MyExecutable`.

□ Wahr
☑ Falsch

What are valid methods to enable a thread-safe for-each loop iteration over a `List myList1`? Hint: consider the case that a second thread attempts to add an item to `myList1` while the loop is still active.

□ a. Creating a thread-safe wrapper with `Collections.synchronizedList(myList1)`.
□ b. There is no need for synchronization. An iteration is only a series of read-accesses.
☑ c. Creating a synchronized block that uses `myList1` as lock-object.

Consider the following class:

```
class Worker {
  void synchronized foo() { /* ... */ }
  void synchronized bar() { /* ... */ }
}
```

Suppose two threads T1 and T2 call the same object `Worker worker = new Worker()`, but T1 calls `worker.foo()` and T2 calls `worker.bar()`. What happens?

☑ a. T1 has to wait for T2 to finish.
□ b. T1 and T2 execute in parallel.

Mark the correct answers regarding data and multithreading:

☑ a. If a Java program with multiple threads runs on a single processor (CPU), the operations of all concurrent threads are executed sequentially. The execution order of these operations is non-deterministic.
□ b. The JVM automatically performs synchronization where multiple threads try to manipulate data.
☑ c. The programmer has to ensure that concurrent access to data by multiple threads is synchronized.

□ d. Objects that are passed into other threads are automatically passed as deep copies to ensure thread safety.

Which of these code snippets are valid ways of implementing a thread-safe, consistent, and atomic in-memory ID generator?

□ a. A:

```
class IdGenerator {
  int id = 0;
  int next() {
    id = id + 1;
    return id;
  }
}
```

□ b. B:

```
class IdGenerator {
  int id = 0;
  int next() {
    return ++id;
  }
}
```

☑ c. C:

```
class IdGenerator {
  AtomicInteger id = new AtomicInteger();
  int next() {
    return id.incrementAndGet();
  }
}
```

☑ d. D:

```
class IdGenerator {
  int id = 0;
  int synchronized next() {
    return ++id;
  }
}
```

What happens when the shutdown method of `java.util.concurrent.ExecutorService` is called?

□ a. All threads submitted to the executor are terminated.
□ b. The thread running the executor is terminated.
☑ c. The executor stops accepting new submit requests.
□ d. The method blocks until all threads submitted to the executor have finished.

RMI

Invocations to remote objects via RMI are thread safe.

- □ Wahr
- ☑ Falsch

Which types of exceptions can be used in the `throws` clause of remote object methods in RMI?

- □ a. Only exceptions that extend from `java.rmi.RemoteException`.
- ☑ b. Any exception that extends `java.lang.Exception`.
- □ c. Only exceptions that extend from `java.lang.RuntimeException`.
- □ d. RMI does not support custom exceptions.

Java RMI communication is encrypted.

- □ Wahr
- ☑ Falsch

Which types of objects can be passed as parameters to a method defined by an RMI remote object (suppose both client and server have access to the same code).

- ☑ a. Any primitive data type.
- □ b. Any object that does not use other complex types (like collections).
- ☑ c. Any fully serializable object.
- □ d. Any object that only has primitive members.
- ☑ e. References to other remote objects.

As soon as a remote object is exported, it can be found in the RMI registry.

- □ Wahr
- ☑ Falsch

Which statements about Java RMI are correct?

- ☑ a. It allows programs running in different Java Virtual Machines to communicate.
- ☑ b. It is the object-oriented equivalent of remote procedure call (RPC).
- □ c. It simplifies security mechanism.
- □ d. It simplifies data exchange between programs written in different languages.

Which statements about Java RMI are correct?

- ☑ a. It is the object-oriented equivalent of remote procedure call (RPC).
- □ b. It relies on the publish/subscribe messaging pattern.
- □ c. It simplifies the coordination of multi-threaded programs.
- ☑ d. It simplifies data exchange between Java programs.

Which statements about Java RMI are correct?

☑ a. It allows programs running in different Java Virtual Machines to communicate.
☐ b. It is the object-oriented equivalent of TCP.
☑ c. It is an API to hide network communication from the programmer.
☐ d. It simplifies data exchange between programs written in different languages.

In RMI for bootstrapping purposes you have to register with the RMI registry ...

☐ Wahr
☑ Falsch

If an object is an instance of `java.rmi.server.UnicastRemoteObject` then it also implements `java.io.Serializable`.

☑ Wahr
☐ Falsch

Assume a remote interface `MyRemoteA` and another remote interface `MyRemoteB` that declares a method with the signature `void foo(MyRemoteA a) throws RemoteException;`. Is the method signature of `foo` a valid signature for an RMI remote method?

☑ Wahr
☐ Falsch

How can you make an object which implements `java.rmi.Remote` remotely accessible through RMI?

☑ a. I let its class extend `java.rmi.remote.UnicastRemoteObject`.
☐ b. It is already remotely accessible, because of the implemented `java.rmi.Remote` interface.
☑ c. I use the static `exportObject` method of `java.rmi.remote.UnicastRemoteObject`.
☐ d. It is sufficient to bind the object in the RMI Registry.

Remote objects should be serializable

☑ Wahr
☐ Falsch