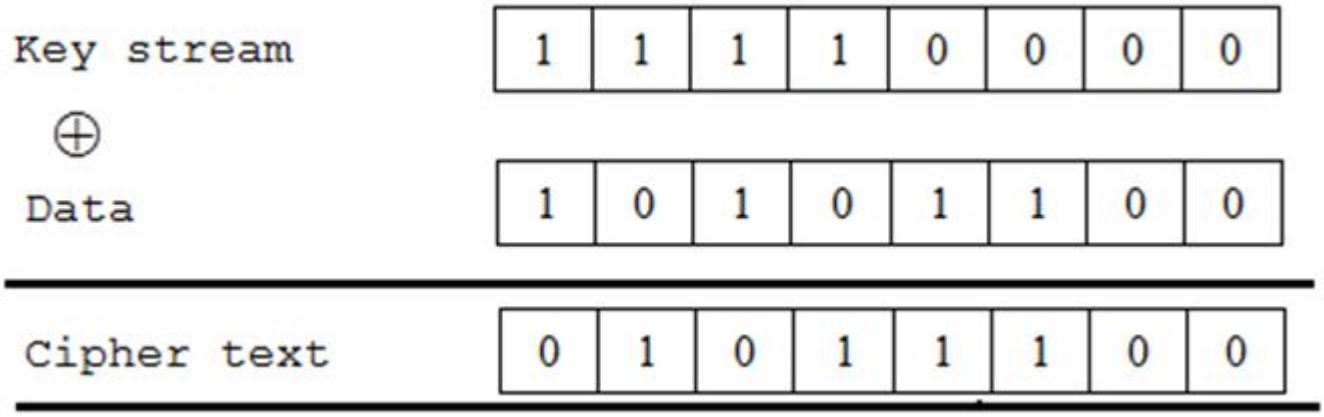
2018S1 9337 midterm quiz

Q1 ?

Consider WEP for 802.11. Suppose that the data is 10001101 and the keystream is 1101010. Which of the following is the resulting ciphertext:

11100111



Q2

Internet Checksum provides better check than a hash function. False

Hash function and checksum function both return a value which cannot be reversed.

An Internet checksum (TCP checksum or IP checksum) is designed to detect common errors quickly and efficiently. An Internet checksum does not attempt to prevent collisions. Man cksum for more info. A Hash provides better message integrity because it has less collisions then an Internet checksum. A collision means there is more then one way to produce the same sum. A great hash function aims to reduce the occurrence of collisions. Man md5 and sha for more info.

What is a collision

Let H() be a hash function. Let x and y be two differing messages. H(x) = H(y) would be a collision.

Q3

The message authentication code HMAC uses: Hash function Correct both "Hash function" and "Cryptographic key".

Q4

The digital signature of a message is The hash of the message encrypted with the private key of the sender.

Q5

Diffie-Hellman and the Digital Signature Algorithm are used to encrypt in SSL applications False

RSA is two algorithms, one for asymmetric encryption, the other one for digital signatures. They use the same kind of keys, they share the same core operation, and they are both called "RSA".

Diffie-Hellman is a key exchange algorithm; you can view it as a kind of asymmetric encryption algorithm where you do not get to choose what you encrypt. This is fine for key exchange, where you just want to obtain an essentially random shared secret between two people. Note that most usages of RSA asymmetric encryption, in practice, are also key exchange, e.g. in SSL/TLS: the client generates a random value, encrypts it with the server's public key, and send it to the server.

PKI is a concept. It builds on the notion of certificate: a certificate is an assertion of key ownership. Basically, a certificate is an object that contains an identity (a name) and a public key, and the object is digitally signed (e.g. with RSA -- the signature algorithm -- or ECDSA). A certificate is validated by verifying this signature. The idea is that if I know the public key of whoever issued (signed) the certificate, then I can verify that signature, and thereby gain some confidence in the fact that the public key contained in the certificate really belongs to the entity designated by the identity contained in the certificate.

When you organize certificates in a way such that there is a strict hierarchy, where certificate issuers are called Certification Authorities and issue certificates to each other, with a handful of top-CA called "root CA", then that overall structure is called a Public Key Infrastructure, i.e. a PKI.

X.509 is a standard for the format and contents of certificates. X.509 is rather open about what signature algorithms will be used for signing certificates, but in practice, 99% of the time, it will be RSA.

Q6

In SSL Protocol, the handshake protocol uses symmetric key cryptography to establish a shared secret key. False
https://www.ibm.com/support/knowledgecenter/en/SSFKSJ_7.1.0/com.ibm.mq.doc/sy10660_.htm Use asymmetric encryption techniques to generate a shared secret key, which avoids the key distribution problem. SSL or TLS then uses the shared key for the symmetric encryption of messages, which is faster than asymmetric encryption.

Q7

The use of public key cryptography is much faster than the use of symmetric key cryptography.

Q8

If a hash function produces a full-length hash value of 512 bits, then the collision resistance is approximately: 256 bits

Security properties of hash functions are generally concerned with collision resistance, but preimage resistance is also important.

For most common hash functions with an n-bit digest size, a successful preimage attack has generic 2n maximum complexity, and a successful collision attack has generic 2n/2 maximum

complexity.

Most common hash functions also use a message block expansion that takes a message block twice the size of its internal state, and the digest size is generally the entire internal state or a truncation. The message is expanded from twice the state to however many bits is required for the rounds. Round input sizes vary with the design, SHA-2 uses a round input that is 1/8 of the internal state. Blake uses the entire message block each round I believe. Other hash functions such as Keccak vary the message block size in order to change the security level. When designing a hash function the message block size can be important for security, and the size is dependent on the design.

The current NIST recommendation is 224-bit digests providing 112-bit resistance against collisions and at least 112-bit resistance against preimages. This recommendation makes several assumptions, notably that the attacker has the resources of a nation state, and that you do not need the hash to be secure for more than a given period of time. These are good assumptions. An additional assumption that is not made, but should be mentioned, is the possibility of undisclosed vulnerabilities that weaken the hash. The round count must be large enough (given round complexity) to prevent a short-cut attack.

If the time the hash needs to be secure exceeds 20 years (as of 2010), more than 112-bits of security are required. 128-bits of security should meet the requirements of all but the most paranoid for the next 35 years. Paranoia (or prudence) could add 6 to 16-bits of security to compensate for potential vulnerabilities or shortcut attacks. 256-bits of security should meet the requirements of anyone, forever (thanks to thermodynamics).

Q9

Suppose Bob initiates a TCP connection to Eve who is pretending to be Alice. During SSL handshake, Eve sends Bob Alice’s certificate. Which of the following statement is true for this scenario

Eve sends to Bob a MAC of all the handshake messages, using a guessed authentication key which is accepted by Bob. The MAC test will fail, and Bob will end the TCP connection.
http://web.cs.du.How SSL and TLS provide authentication
edu/~ramki/courses/security/2010Spring/networkSecurity.pdf

How SSL and TLS provide authentication:

https://www.ibm.com/support/knowledgecenter/en/SSFKSJ_7.1.0/com.ibm.mq.doc/sy10670_.htm

Q10

If an individual signs a message with his private key, this act carries with it non-repudiation. True

A digital signature is a mathematical scheme for demonstrating the authenticity of digital messages or documents. A valid digital signature gives a recipient reason to believe that the message was created by a known sender (authentication), that the sender cannot deny having sent the message (non-repudiation), and that the message was not altered in transit (integrity).

Q11

Which of the following is true regarding WEP cracking?

initialization vectors are small, get reused frequently, and are sent in clear text.

The 802.11 encryption algorithm called WEP (short for Wired Equivalent Privacy) used a short, 24-bit IV, leading to reused IVs with the same key, which led to it being easily cracked.[7] Packet injection allowed for WEP to be cracked in times as short as several seconds. This ultimately led to the deprecation of WEP. The IV is too small and in cleartext. It's a 24-bit field sent in the cleartext portion of a message. This 24-bit string, used to initialize the key stream generated by the RC4 algorithm, is a relatively small field when used for cryptographic purposes.

Q12

Cryptographic hash function takes an arbitrary block of data and returns

fixed size bit string

Q13

RC4 is a _____.Stream cipher

Q14

The security of X.509 as deployed on the WWW is established by

In cryptography, X.509 is a standard that defines the format of public key certificates. X.509 certificates are used in many Internet protocols, including TLS/SSL, which is the basis for HTTPS[1], the secure protocol for browsing the web. They are also used in offline applications, like electronic signatures. An X.509 certificate contains a public key and an identity (a hostname, or an organization, or an individual), and is either signed by a certificate authority or self-signed. When a certificate is signed by a trusted certificate authority, or validated by other means, someone holding that certificate can rely on the public key it contains to establish secure communications with another party, or validate documents digitally signed by the corresponding private key.

Besides the format for certificates themselves, X.509 specifies certificate revocation lists as a means to distribute information about certificates that are no longer valid, and a certification path validation algorithm, which allows for certificates to be signed by intermediate CA certificates, which are in turn signed by other certificates, eventually reaching a trust anchor.

X.509 is defined by the International Telecommunications Union's Standardization sector (ITU-T), and is based on ASN.1, another ITU-T standard.

Q15

If a sender proves his/her identity to the receiver by encrypting a random number by a secret key, then what is the drawback of this scheme? Both parties must be aware of the key

In cryptography and computer security, a man-in-the-middle attack (MITM) is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe

they are directly communicating with each other. One example of man-in-the-middle attacks is active eavesdropping, in which the attacker makes independent connections with the victims and relays messages between them to make them believe they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker. The attacker must be able to intercept all relevant messages passing between the two victims and inject new ones. This is straightforward in many circumstances; for example, an attacker within reception range of an unencrypted wireless access point (Wi-Fi) could insert himself as a man-in-the-middle. [1]

https://en.wikipedia.org/wiki/Man-in-the-middle_attack As an attack that aims at circumventing mutual authentication, or lack thereof, a man-in-the-middle attack can succeed only when the attacker can impersonate each endpoint to their satisfaction as expected from the legitimate ends. Most cryptographic protocols include some form of endpoint authentication specifically to prevent MITM attacks. For example, TLS can authenticate one or both parties using a mutually trusted certificate authority.

https://en.wikipedia.org/wiki/Replay_attack A replay attack (also known as playback attack) is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts the data and re-transmits it, possibly as part of a masquerade attack by IP packet substitution. This is one of the lower tier versions of a "Man in the middle attack."

Another way of describing such an attack is: "an attack on a security protocol using replay of messages from a different context into the intended (or original and expected) context, thereby fooling the honest participant(s) into thinking they have successfully completed the protocol run." [1]

Q16

In SSL record, there is a field called sequence number that is to protect a session from replay attack. False

In SSL/TLS handshake, a nonce is always sent by the client to server and vice versa. The nonce basically consists of a random number and unix timestamp.

https://www.ibm.com/support/knowledgecenter/SSB23S_1.1.0.12/gtps7/s5rcd.html

```
There are three record types for SSL version 3 and TLS
version 1:
    Handshake
    Alert, which is a warning or fatal error
    Data (application data).
The data in the record has the following characteristics:
    A variable length and starts with a 5-byte record header
    Contains handshake data, alert data, or application data
    Is encrypted, except for the first SSL handshake flows
The message digest has the following characteristics:
    A fixed length that is based on the digest algorithm used
    Is included only if the data is encrypted
```

Q17

SSL/TLS uses two protocols. It first uses the record protocol and then the handshake protocol. False

The TLS protocol comprises two layers: the TLS record and the TLS handshake protocols.

Q18

A message digest can be inverted to obtain the original message. False

Q19

In Diffie-Hellman key exchange protocol if the private key of Alice and Bob are, a = 6 and b = 15 resp. and g= 5 and p= 23, then the public key of Alice (A) and Bob (B) and shared secret key are: A= 8, B = 19, S=2

Q20

From your knowledge of security protocols at Transport layer, when shopping at amazon.com, the client's credit card number is encrypted by

A symmetric key established in the handshake protocol.

The connection is private (or secure) because symmetric cryptography is used to encrypt the data transmitted. The keys for this symmetric encryption are generated uniquely for each connection and are based on a shared secret negotiated at the start of the session (see § TLS handshake). The server and client negotiate the details of which encryption algorithm and cryptographic keys to use before the first byte of data is transmitted (see § Algorithm below). The negotiation of a shared secret is both secure (the negotiated secret is unavailable to eavesdroppers and cannot be obtained, even by an attacker who places themselves in the middle of the connection) and reliable (no attacker can modify the communications during the negotiation without being detected).

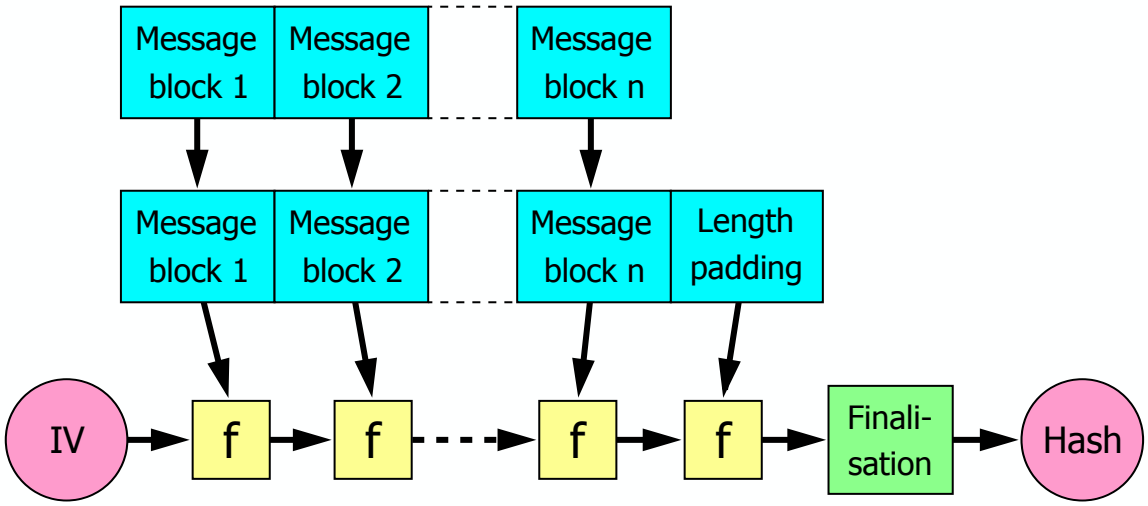
Once the client and server have agreed to use TLS, they negotiate a stateful connection by using a handshaking procedure.[6] The protocols use a handshake with an asymmetric cipher to establish not only cipher settings but also a session-specific shared key with which further communication is encrypted using a symmetric cipher. During this handshake, the client and server agree on various parameters used to establish the connection's security

Q21

When an initialization vector is used as an input in the encryption process, it must always be a secret. False https://crypto.stackexchange.com/questions/3965/what-is-the-main-difference-between-a-key-an-iv-and-a-nonce?utm_medium=organic&utm_source=google_rich_qa&utm_campaign=google_rich_qa A key, in the context of symmetric cryptography, is something you keep secret. Anyone who knows your key (or can guess it) can decrypt any data you've encrypted with it (or forge any authentication codes you've calculated with it, etc.).

(There's also "asymmetric" or public key cryptography, where the key effectively has two parts: the private key, which allows decryption and/or signing, and a public key (derived from the corresponding private key) which allows encryption and/or signature verification.)

An IV or initialization vector is, in its broadest sense, just the initial value used to start some iterated process. The term is used in a couple of different contexts, and implies different security requirements in each of them. For example, cryptographic hash functions typically have a fixed IV, which is just an arbitrary constant which is included in the hash function specification and is used as the initial hash value before any data is fed in:



In any case, the IV never needs to be kept secret — if it did, it would be a key, not an IV. Indeed, in most cases, keeping the IV secret would not be practical even if you wanted to, since the recipient needs to know it in order to decrypt the data (or verify the hash, etc.).

Q22 ?

Consider a security protocol where the sender sends (m, H(m)+s), where , H(m)+s is the concatenation of H(m) and s. H() being the hash function, m the message and s the secret key. This is scheme is clearly flawed because:

An attacker can sniff and obtain shared secret

Q23

The initialization vector (IV) appended to the secret symmetric key in WEP protocol is encrypted before sending to the receiver False

Q24

Evan has configured a laptop and an AP, each with two WEP keys. WEP key 1 is the same on both devices, and WEP key 2 is the same on both devices. He configured the laptop to use WEP key 1 to encrypt its data. He configured the AP to use WEP key 2 to encrypt its data. Will this configuration work?

Yes, as long as the value of WEP key 1 is identical on both computers and the value of WEP key 2 is identical on both computers.

Up to four WEP keys can be entered on a Wi-Fi device. In addition to four WEP keys being entered, one will be designated to be used to encrypt all transmitted data. When the encrypted frame is received, part of the frame tells the receiving system which key (1, 2, 3, or 4) was used to encrypt the frame. The receiving system then attempts to decrypt the frame using the speci ed key. If the value of the key is the same on the receiving system, then the frame will be decrypted. Each system can use a separate key to encrypt the data.

Q25

Triple DES has an effective _____-bit key. 56