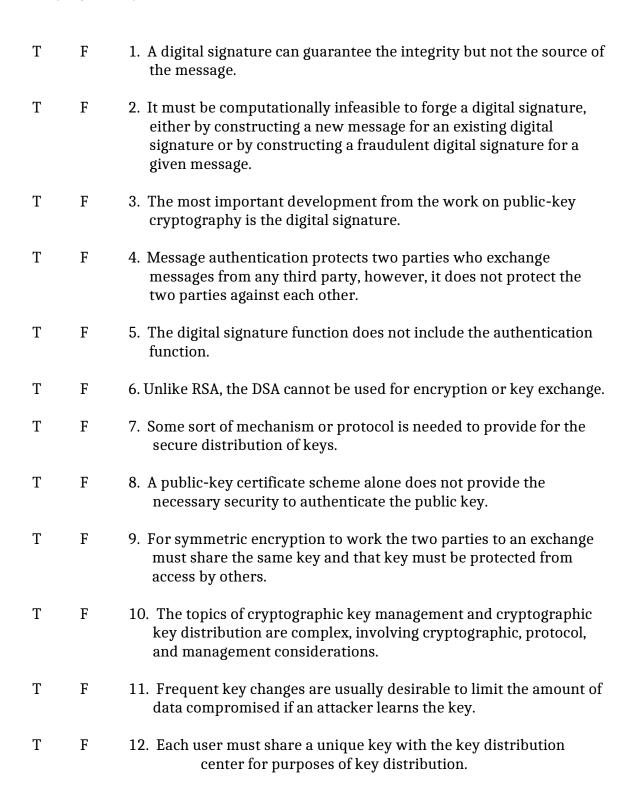
## DIGITAL SIGNATURES & KEY DISTRIBUTION

## TRUE OR FALSE



T F 13. Typically the session key is used for the duration of a logical connection, such as a frame relay connection or transport connection, and then it is permanently stored. T F 14. Master keys can be distributed in some non-cryptographic way such as physical delivery. MULTIPLE CHOICE 1. The \_\_\_\_\_ is formed by taking the hash of the message and encrypting the message with the creator's private key. B. message digest A. timestamp C. hash code D. digital signature 2. \_\_\_\_\_ is where the attacker forges a signature for a particular message chosen by the attacker. A. Total break B. Universal forgery C. Existential forgery D. Selective forgery 3. The digital signature standard is a \_\_\_\_\_ standard that uses the secure hash algorithm. A. IEEE B. NIST C. ISO D. ITIL 4. With a \_\_\_\_\_ attack the attacker is given access to a set of messages and their signatures. A. known message B. key-only C. directed chosen message D. generic chosen message

5.	A is where the attacker d	etermines the user's private key.
	A. universal forgery	B. selective forgery
	C. existential forgery	D. total break
6.	Key distribution often involves the used and are long lasting.	e use of which are infrequently
	A. private key certificates	B. master keys
	C. session keys	D. public key certificates
7.	key encryption schemes authenticated.	are secure if the public key is
	A. Message	B. Management
	C. Public	D. Private
8.	A defines the procedures	needed to revoke digital certificates.
	A. KDC	B. digital key
	C. cryptographic key encryption	D. public key infrastructure
9.	Key distribution often involves the distributed for temporary use between	e use of which are generated and ween two parties.
	A. public key certificates	B. session keys
	C. master keys	D. private key certificates
10	. If is done at a network or hosts on the network that wish to	IP level a key is needed for each pair of communicate.
	A. end-to-end encryption	B. key management
	C. key distribution	D. link encryption

11	. Communication between e	nd systems is encrypted using a key.
	A. session	B. master
	C. permanent	D. message
12		on keys are exchanged the more they are ess ciphertext to work with for any given session
	A. insecure	B. streamlined
	C. secure	D. obsolete
13	. One of the most important secret keys for distribution	uses of a cryptosystem is to encrypt
	A. master key	B. KDC
	C. public key	D. end-to-end
SHOR	T ANSWER	
1.		ent signing algorithm that provides an equivalent ares on arbitrary messages is a
2.	author and the date and tin	ve the following properties: it must verify the ne of the signature; it must authenticate the signature; and it must to resolve
3.	The DSS makes use of the S signature technique known	ecure Hash Algorithm and presents a new digital as the
4.	attempting to break the use	re the attacker chooses a list of messages before er's signature scheme, independent of the user's en obtains from the user valid signatures for the
5.	The term refers to	a digital signature scheme that involves only the

## COMP-424 November 15, 2016

6.	communicating parties is the function that delivers a key to two parties who wish to exchange secure encrypted data.
7.	A is defined as the set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates based on asymmetric cryptography.
8.	Used in a variety of applications, defines the format for public-key certificates.
9.	Public-key encryption schemes are secure only if the authenticity of the is assured.
10.	If encryption is done at the level a key is needed for every pair of users or processes that require communication.
11.	If A and B each has an encrypted connection to a third party C, C can deliver a key on the encrypted links to A and B. A is responsible for distributing keys to pairs of users as needed.
12.	Session keys are transmitted in encrypted form using a that is shared by the key distribution center and an end system or user.