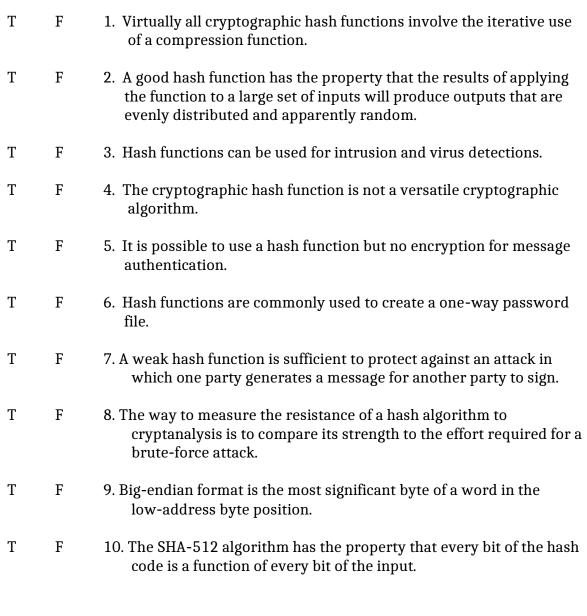
CRYPTOGRAPHIC HASH FUNCTIONS

TRUE OR FALSE



MULTIPLE CHOICE

1. The principal object of a hash function is	
---	--

A. data integrity

B. compression

	C. collision resistance	D. mapping messages		
2.	A accepts a variable length fixed size hash value $h = H(M)$.	th block of data as input and produces a		
	A. hash resistance	B. hash value		
	C. hash function	D. hash code		
3. A is an algorithm for which it is computationally infeasible to f either (a) a data object that maps to a pre-specified hash result or (b) tw data objects that map to the same hash result.				
	A. cryptographic hash func	tion B. strong collision resistance		
	C. one-way hash function	D. compression function		
4.	I. The cryptographic hash function requirement that guarantees that it is impossible to find an alternative message with the same hash value as a given message and prevents forgery when an encrypted hash code is used ithe			
	A. collision resistant	B. pseudorandomness		
	C. pre-image resistant	D. second pre-image resistant		
5.	is a mechanism or service	e used to verify the integrity of a message.		
	A. Message authentication	B. Data compression		
	C. Data mapping	D. Message digest		
6.	Message authentication is achieved	d using a		
	A. DES	B. MDF		
	C. SHA	D. MAC		
7.	are measures of the num value.	ber of potential collisions for a given hash		

	A.	MACs	В. І	Primitives
	C.	Hash codes	D. 1	Preimages
8.	output si	<u>-</u>	-	erties of variable input size, fixed and second preimage resistant is
	A.	strong hash function		B. collision resistant function
	C.	weak hash function		D. preimage resistant function
9.		rt required for a collision r atical result referred to as		tant attack is explained by a
	A.	Whirlpool	B. ł	oirthday paradox
	C.	hash value	D. 1	message authentication code
10	An ideal force effo	_	e a c	eryptanalytic effort the brute
	A.	less than or equal to		B. greater than or equal to
	C.	less than		D. greater than
11.	. SHA-1 pr	oduces a hash value of		bits.
	A.	. 224	В. 1	160
	C.	384	D. 2	256
12.	H is appl	ied to k random inputs, whity that at least one input y	hat r	le outputs and a specific value $H(x)$, if must be the value of k so that the isfies $H(y) = H(x)$ is 0.5?" is a reference
	A.	authentication code		B. collision resistant
	C.	big endian		D. birthday attack

13		w versions of SHA wetively known as	vith hash value lengths of 256, 384, and 512 bits
	A.	SHA-3	B. SHA-1
	C.	SHA-2	D. SHA-0
SHOR	T ANSWE	R	
1.	two cate		sed in secure hash algorithms falls into one of pecifically designed for the hash function or an
2.	Aalgorithm		l on weaknesses in a particular cryptographic
3.		•	ntees that it is impossible to find an alternative value as a given message.
4.		of hash function ned hash function.	eded for security applications is referred to as a
5.	The most is the	important and wid	ely used family of cryptographic hash functions
6.			d to provide message authentication, the hash red to as a
7.	-	nents for a cryptogra vay property.	aphic hash function include which is
8.	output si	ze, efficiency, preim	s the properties of variable input size, fixed age resistant, second preimage resistant and trong hash function.

9.	The two categories of attacks on hash functions are attacks and cryptanalysis.
10.	The evaluation criteria for SHA-3 are security,, and algorithm and implementation characteristics.
11.	A message authentication code is also known as a hash function.
12.	The hash value of a message in the application is encrypted with a user's private key.
Questi	ons

- What are some approaches to producing message authentication?
 Compare message hashes and MACs