

Name \_\_\_\_\_

## Matching

Select the most correct answer from Table 1-2 and place the letter of the answer in the ANSW column.

ANSW	#	Term
	1.	Protocol
	2.	Authentication
	3.	Secret splitting
	4.	Algorithm
	5.	Block Cipher
	6.	Block Chaining
	7.	Cipher
	8.	Clustering
	9.	Codes
	10	Cryptanalysis
	.	
	11	Ciphertext
	.	
	12	Decryption
	.	
	13	Key
	.	
	14	Keyspace
	.	
	15	Key clustering
	.	
	16	Link Encryption
	.	
	17	Plaintext
	.	
	18	Stream cipher
	.	
	19	Passphrase
	.	
	20	Stenography
	.	
	21	Work Function (factor)
	.	

Table 1-1, Matching Questions

**Answers**

##	Definition
a.	Range of values that can be used to construct a key.
b.	Sequence of bits and instructions that governs encryption and/or decryption.
c.	When a plaintext message generates identical ciphertext messages using the same transformation algorithm.
d.	Changing ciphertext back to plaintext.
e.	In the transmission chain, where each entity has keys in common with its two neighboring nodes.
f.	Data that can be read and understood without any special measures aka cleartext.
g.	Plaintext that has been encrypted.
h.	The science of analyzing and breaking secure communication..
i.	Message broken into characters or bits and enciphered with a key stream. (Contrast with block cipher.)
j.	A cryptographic transformation that operates at the level of words or phrases.
k.	Situation when a plain text message generates identical cipher text messages using the same transformation algorithm.
l.	A sequence of words, or text, used to control access to a computer system, program or data.
m	An agreed-upon sequence of actions performed by two or more principals
.	
n.	A method that encrypts or disguises text.
o.	Secret communications where the existence of the message is hidden.
p.	Parts of previous block are inserted into current block
q.	Measure of difficulty in recovering plaintext from cipher text. AKA encryption method strength. Measured in bits.
u.	Process of proving your identity to someone else
r.	A well-defined procedure or sequence of steps used to produce a key stream or cipher text from plain text
s.	Divide a message into n pieces, such that all n pieces must be combined to recover the message
t.	Obtained by segmenting plaintext into fixed size blocks and applying the identical encryption algorithm to each block

Table 1-2, Answers