Task 10. Read the text below and decide which answer (A, B, C or D) best fits each gap.

Text C.Coding Theory

Coding theory is the study of properties of codes It is a _____ **(1)** of mathematics concerned with transmitting data across noisy channels and recovering message. Codes are studied by various scientific _____ **(2)**such as information theory, electrical engineering, mathematics, linguistics, and computer science.

There are four types of coding: data compression (or *source coding*), error correction (or *channel coding*), cryptographic coding and line coding.

Data compression attempts to compress the data from a source in order to transmit it _____ **(3)**efficiently. For example, Zip data compression makes data files smaller to _____ **(4)** Internet traffic. Data compression and error correction may be studied in combination.

Error correction adds extra data bits to _____ **(5)**the transmission of data more robust to disturbances present on the transmission channel. The ordinary user may not be _____ **(6)**of many applications using error correction. A typical music CD uses the Reed-Solomon code to correct for scratches and dust. In this application the transmission channel is the CD itself. Cell phones also use coding techniques to correct for the fading and noise of high frequency radio transmission. Data modems, telephone transmissions, and NASA all _____ **(7)**channel coding techniques to get the bits through.

Coding theory is one of the most important and direct applications of information theory. Concepts, methods and results from coding theory and information theory are _____ **(8)**used in cryptography and cryptoanalysis.

1	A	segment	B	branch	C	field	D	sector
2	A	subjects	B	sciences	C	disciplines	D	objects
3	A	more	B	most	C	less	D	least
4	A	lessen	B	shorten	C	lengthen	D	reduce
5	A	help	B	do	C	create	D	make
6	A	aware	B	Know	C	conscious	D	recognise
7	A	exploit	B	employ	C	get	D	choose
8	A	usually	B	commonly	C	widely	D	deeply

Task 11. Read the text below. Choose from (A-H) the one which best fits the space (1-8). There are two choices you do not need to use.

Text D. The Unbreakable Code

A. to encode the message with a random series of digits
B. as well as defining information
C. that unbreakable cryptography was possible
D. the amount of uncertainty we can introduce
E. because they merely relabel the characters

F. and the resulting transformation may be considered a cipher
G. no other encryption scheme
H. called 'a key' to help encrypt and decrypt messages

A year after Claude Elwood Shannon founded and launched information theory, he published another notable paper called 'Communication Theory of Secrecy Systems', which proved **(1)**_____. In particular, he began his analysis by noting that simple transposition ciphers – such as those obtained by permuting the letters in the alphabet – do not affect the entropy **(2)**_____ in his formula without changing their associated probabilities.

The scheme is called 'the one-time pad' or 'the Vernam cipher', after Gilbert Vernam, who had invented it near the end of World War I. The idea is **(3)**_____ – the key – so that the encoded message is itself completely random.The catch is that the person who encodes the message needs a random key, and this key must never be used twice.

Cryptographic systems employ special information **(4)**_____. Sometimes different keys are used both for the encoding and decoding, while in other instances, the same key is used for both processes. Shannon made the following general observation: "**(5)**_____ into the solution cannot be greater than the key uncertainty." This means, among other things, that random keys should be selected to make the encryption more secure. While Shannon's work did not lead to new practical encryption schemes, he did supply a framework for understanding the essential features of any such system.

Shannon's contribution was to prove that this code was unbreakable. To this day, **(6)**_____ is known to be unbreakable.

Task 12. Fill in the gaps in the of-phrases below with the words from the box. All the phrases can be found in the texts above.

chance	branch	mode	arrangement
Institute	transmission	properties	amount
rate	series	dawn	number

1. _____ of signals
2. the _____of information
3. the _____ of binary digits
4. every _____ of communication
5. the _____ of the information age
6. Massachusetts _____of Technology
7. the _____ of the relays
8. the minimum _____ of a source code
9. arbitrarily small _____ of error
10. _____of codes
11. a _____of mathematics
12. a random _____ of digits