1. Be familiar with the text, from the section *Agony Columns to Buried Treasure* of chapter 2 to the end of chapter 3.

2. Explain how Alberti's bi-alphabetic cipher works. Explain how you would crack Alberti's bi-alphabetic cipher, assuming each alphabetic permutation came from a keyphrase.

3. Define index of coincidence. Define index of mutual coincidence.

4. Explain the Babbage/Kasiski method for cracking the Vigenere cipher. Explain the Friedman method for cracking the Vigenere cipher.

5. What kind of agony is involved in an agony column? What cipher system is credited to Aeneas Tacticus?

6. Define cryptolit. It is harder to crack the cipher in Sayers' novel *Have his carcase* than the cipher in Poe's novel *The Gold Bug*. Why is this not surprising?

7. Explain how the book cipher works. Explain the role of textual analysis in giving evidence that the Beale saga is a hoax.

8. What is a Morse fist? Explain how it was used together with triangulation to track movement of German battalions by the French in WWI. Explain why this method was not used by the Germans to track movement of French battalions by the Germans.

9. What is a Polybius grid? Why was it invented? Explain how the Playfair cipher works.

10. Explain how the ADFGVX cipher works. Why does the ADFGVX cipher use the letters ADFGVX and not the letters ABCDEF? Explain how to crack the ADFGVX cipher.

11. Why did America not enter the war after the Germans sank the passenger freighter Lusitania in 1915 ? How did Zimmermann plan to keep America from contributing to the Allies in WWI? Was the Zimmermann telegram sent by wire or by radio? Why? How did the Brits come to be in possession of the encrypted Zimmermann telegram? In the telegram, what did the Germans offer the Mexicans? What was Room 40? After the Allies came into posession of the decrypted telegram, why did the Germans not realize that their system had been cracked? What did the British think Zimmermann would say when asked by the press about the telegram?

12. In what sense is the 1-time pad the holy grail of cryptography? In what sense is the 1-time pad unbreakable? Give three issues of concern when using the 1-time pad.

13. What is the running key cipher? How does it differ from the 1-time pad? How can it be broken? Explain how to break a twice used 1-time pad.

14. Explain what the keyboard, plugboard, scramblers, reflectlor, lampboard each do in the Enigma. Explain how the reflector helps the Enigma's ease of use. Explain why the number of different scrambler orientations is 17,576. Explain why the number of different plugboard settings (with 12 cables) is around 10^{11}. Explain how Churchill's book *The World Crisis* led to increased sales for the Enigma.