1. انواع تهدیدات امنیتی را نام ببرید و هریک را تعریف کنید.(3مورد)
2. موارد زیر را تعریف کنید:
	1. حمله
	2. نقطه اسیب پذیر
3. خدمات امنیتی را نام ببرید و هر یک را توضیح دهید(5 مورد)
4. موارد زیر را تعریف کنید
	1. استراق سمع
	2. دستکاری
	3. جعل
	4. وقفه
5. حملات فعال و غیر فعال را تعریف کنید.
6. اصول ششگانه کرکهف را بیان کنید
7. رمز نگاری متقارن را توضیح دهید
8. رمزنگاری کلید عمومی را توضیح دهید
9. منظور از رمزشکنی چیست
10. رمز شکنی «صرفا متن رمز شده» یا cipherText-Only را شرح دهید
11. رمز شکنی «متن شناخته شده و اشکار» یا Known-Plaintext را شرح دهید
12. رمز شکنی «متن انتخابی و شناخته شده » یا Chosen-Plaintext را شرح دهید
13. اصول رمزنگاری زیر را شرح دهید
	1. استحکام
	2. تازگی
	3. افزونگی
14. نقاط ضعف هر یک از روش های زیر را بیان کنید
	1. رمز سزار
	2. جانشینی تک حرفی
	3. رمز نگاری دوحرفی Playfair
	4. رمزنگاری چند حرفی هیل
	5. رمزنگاری one-time-pad
15. روش رمز نگاری one-time-pad را شرح دهید
16. جعبه جایگشت یا P-BOX را شرح دهید
17. جعبه جانشینی یا S-BOX را شرح دهید
18. ویزگی های بنیادین سیستم های مدرن رمز نگاری را نام ببرید
19. هریک از موارد زیر را شرح دهید
	1. پخش و پراکنده سازی
	2. گمراه کنندگی
	3. اثر فروپاشی بهمنی
	4. برابری طول خروجی و ورودی
20. معماری فیستلی را با رسم شکل شرح دهید
21. الگوریتم رمز نگاری DES را با رسم شکل شرح دهید
22. تفوت الگوریتم DES و 3DES را شرح دهید
23. الگوریتم 3DES را شرح دهید
24. چهار عملکرد اصلی درون الگوریتم AES را بیان کنید
25. شیوه کتابچه رمز را شرح دهید
26. زنجیره سازی بلوکهای رمز CBC را با رسم شکل توضیح دهید.
27. ویژگی انتشار رو به جلو چیست
28. ویژگی انتشار خطا چیست
29. شیوه فیدبک (feedback) را به کمک رسم نمودار توضیح دهید
30. رمزنگاری به شیوه استریم را توضیح دهید
31. رمز نگاری به شیوه شمارنده را با رسم شکل توضیح دهید.
32. دلایل استفاده از شیوه رمز زنجیره بلوک داده چیست
33. رمزنگاری به شیوه شمارنده به چه منظور ارائه شده است.
34. کلید عمومی و کلید خصوصی را شرح دهید
35. الگوریتم RSA را بنویسید.