#	سوالات	بارم
۱	الگوریتم HMAC و اهداف طراحی آن را توضیح دهید و ساختار(شکل) آن را رسم کنید.	
۲	از جمله حملات امنیتی فعال[1] و غیر فعال[2] را شرح دهید و برای هرکدام دو نمونه تشریح کنید.	
۳	یکپارچگی داده[3] را تشریح کرده و سه مورد از سرویس‌های آن را توضیح دهید.	
۴	الگوریتم رمزنگاری AES را شرح‌دهید (اندازه کلید، تعداد دورها، گام‌های هر دور و توضیح هرگام).	
۵	از مودهای علمیاتی رمزهای قالبی، ساختار(شکل) مود زنجیره‌ای قالبی[4] و مود شمارنده[5] را رسم کنید.	

1 Active
2 Passive
3 Data Integration
4 Cipher Block Chaining
5 COUNTER (CTR)