ブロック暗号には、DESとAESがある。DESとは、1977年に採用された共通暗号方式によるデータ暗号化のアルゴリズムである。仕組みとしては入出力長64biを半分に分割して、基本変換のファイステル構造を16回繰り返す。これにより安全性の高い暗号化方法として採用されていたが、秘密鍵長56bitと短く総当たり攻撃に弱いことが判明し、2005年に役目を終えた。その後継機として登場したのが、2001年に採用された、AESが採用された。AESでは鍵長が128bit、192bit、265bitから選べることができる。また、暗号化と復号の処理が異なるSPN構造で基本転換を10回、12回、14回繰り返すのでセキュリティが強いと言われている。AESには、ECBモードとCBCモードがある。EBCモードでは、メッセージブロックの値が同じであれば暗号文ブロックも同じなので、解読されやすい。CBCモードでは、暗号文の各bitをXOR演算して暗号させ、そこで生成された暗号文ブロックは次のブロックの入力に影響するので、メッセージブロックの値が同じでも、暗号文ブロックは異なることによりEBCモードよりも安全ということがわかった。

公開鍵暗号では、共通鍵暗号のような通信相手の数だけ秘密鍵が必要なく、自分の秘密鍵だけを管理すれば良いので、多くの人と暗号通信するときに、鍵管理が容易になる。公開鍵を使用している暗号方式としてRSA暗号があり、大きな数の素因数分解の困難性に基づいているが、同一公開鍵による二つの異なる暗号文の積は対応する平文の積の暗号文になっているため、暗号文の解読は困難であるが、情報セキュリティの世界では、セキュリティ的に弱いとされていることを知ることができた。

ハッシュ関数とは、データの特徴値を算出する衝突を起こしにくい一方向性圧縮関数で、任意長の入力に対してそのデータを代表する固定長の値を出力している。また、ハッシュ関数コンペがあり、SHA１、SHA２、SHA３があるが、現代ではSHA２のSHA-256のハッシュ関数がよく使われている。SHA-256とは、任意の長さのデータから256bitのハッシュ値を生成することができる。また同じデータからは同じ値を得られ、少し違うデータからは違う値が得られるので、データの改ざんされていないかを確認することができることを理解した。ハッシュ関数はブロックチェーンでも利用されているので深く勉強しようと思う。