第14回課題

E1832 藤村勇仁

問1

Q1

私のPCの動作周波数は???で価格は???円。よって、1000万円で???台が使用可能である。$$ \frac{2^{64}}{(60 \times 60 \times 24 \times 365) \times clock \times num} = ??? $$ より、???年である。

Q2

$$ (60 \times 60 \times 24) \times (clock \times 2^n) \times num = 2^{64} \ n = ??? $$ より、???年で1日以内に買得可能になる。

問2

1. デジタル署名では、送信者と受信者で認証機関によって発行された公開鍵が共有されそれによってハッシュ値を復号化するため、送信者を偽ることができない。また、それに伴い情報の盗聴、改ざんなども防止される。
2. デジタル署名はだれが送信したかを保証するためのものである。デジタル署名においてハッシュ値は秘密鍵を用いて暗号化され、公開鍵を用いて復号される。このとき公開鍵で復号できたなら、送信元はそれと対になる秘密鍵であることが保証される。

問3

m=765, p=43, q=79, n=pq=3397 である。$$ (43-1)\times(79-1)=3276=13\times7\times3^2\times2^2 $$ より、eをこれと互いに素な自然数29とすると、$$ ed \bmod (43-1)\times(79-1)=1 $$ となるようなdは113である。

暗号化する際は、暗号文yは、$$ y = m^e \bmod n = 1181 $$ で求められ、復号する際は、$$ m = y^d \bmod n = 765 $$ で求められる。

問4

誤り訂正符号とは、データを記録・伝送する際に発生する誤りを受け手の側で検出し、訂正することができるように付加される符号のこと。元のデータから一定の手順に基いて算出し、データと共に記録・伝送する。(e.g. パリティ検査符号)

暗号とは、悪意のある第三者、つまり攻撃者がいる所でも安全な通信を提供するものである。暗号では、アルゴリズムと鍵を使用して、入力（プレーンテキスト）を暗号化された出力（暗号文）に変換する。