（注意）　各問いの答えは、答案用紙の指定された枠内に収まるようにまとめよ。
（計算等で枠外を用いても良いが、枠外のものは採点の対象とはしない。）

［問1］ 情報セキュリティの 3 要素（CIA）を挙げ、それぞれの内容を説明せよ。［15 点］

［問2］ 情報理論的に安全な暗号と計算量的に安全な暗号との違いを説明せよ。［10 点］

［問3］ 共通鍵暗号と公開鍵暗号のハイブリッド方式において、共通鍵暗号と公開鍵暗号のそれぞれの暗号方式で何を暗号化するかを説明せよ。［10 点］

［問4］ $(3,n)$しきい値秘密分散法によって分散された情報のうち、次の 4 人分の情報が得られた。各情報$(i,f(i))$から秘密を復元せよ。ただし、$f(i)$の計算に用いる素数は13とし、秘密の復元過程も示せ。［15 点］

$(1,1),\quad (4,9),\quad (5,2),\quad (6,1)$

［問5］ RSA 暗号の鍵生成において、二つの素数として13と19を選び、公開鍵を$(31,247)$とした場合の秘密鍵を求めよ。ただし、導出過程も示せ。［20 点］

［問6］ DH(Diffie-Hellman)鍵共有について、次の各問いに答えよ。なお、鍵共有の参加者は、大きな素数pおよび、巡回群$\mathbb{Z}_p^*$の生成元gをあらかじめ共有しているものとする。また、巡回群の演算は$\bmod p$上での乗算とする。［30 点］

(1) 鍵共有の手順を示せ。

(2) CDH(Computational Diffie-Hellman)問題とは何かを説明せよ。

(3) CDH 問題が容易に解けると仮定した場合に、通信路を盗聴して得られる情報のみから鍵共有にて生成する秘密鍵を計算できることを示せ。

（注意）　各問いの答えは、答案用紙の指定された枠内に収まるようにまとめよ。
（計算等で枠外を用いても良いが、枠外のものは採点の対象とはしない。）

［問1］ メッセージMおよびMに対する署名σとして$(M,\sigma)=(37,11)$を入手した。署名を検証せよ。なお、σは RSA 署名方式を用いて生成されているものとし、署名者の公開鍵は$(23,119)$、秘密鍵は$(71,119)$とする。また、署名生成時にハッシュ関数は用いていないものとする。［20 点］

［問2］ バイオメトリック認証について各問いに答えよ。［20 点］

(1) バイオメトリック認証で用いられる生体的特徴が満たすべき条件を一つ挙げ、その内容を説明せよ。

(2) FRR（False Rejection Rate）と FAR（False Acceptance Rate）がそれぞれ何かを説明せよ

［問3］ 電子透かしとステガノグラフィのそれぞれにおいて、重要視される技術要件を説明せよ。［10 点］

［問4］ 認証（authentication）と認可（authorization）がそれぞれ何かを説明せよ。［10 点］

［問5］ マルウェアについて各問いに答えよ。［20 点］

(1) マルウェアとは何かを説明せよ。

(2) ランサムウェアの特徴とその対策を説明せよ。

［問6］ 次に挙げるものが何かを説明せよ。［20 点］

(1) 情報セキュリティポリシー

(2) プライバシー権