

-
1. ゼロ知識対話証明に関する以下の問いに答えなさい。
 - (a) ゼロ知識とはどのような意味か．簡単に説明しなさい．
証明者の有する秘密情報に関する知識が全く漏れないこと．
 - (b) 対話証明とはどのような意味か．簡単に説明しなさい．
証明者と検証者の間で取り決めた手続き (プロトコル) に従って，やり取りをすることにより証明するということ．
 - (c) ゼロ知識対話証明の利点は何か．簡単に示しなさい．
証明者の有する秘密情報が全く漏れずに秘密情報を有していることを示すことができること．
-

(注) 上記はあくまでも略解です．詳しくは講義中に話した内容を参照してください．
