EE309 - Assignment 5

Due - 12/15

Problem 1: Classic cryptography (25pt)

A mono-alphabetic cipher (aka simple substitution cipher) is a substitution cipher where each letter of the plain text is replaced with another letter of the alphabet. It uses a fixed key which consist of the 26 letters of a "shuffled alphabet".

For this example, let's define our substitution as follows:

- Original Alphabet: ABCDEFGHIJKLMNOPQRSTUVWXYZ
- Substituted Alphabet: QWERTYUIOPASDFGHJKLZXCVBNM

if we encrypt "HELLO WORLD", it becomes "ITSSG VGKSR" using this substitution scheme.

This is our text encrypted with an unknown substitution. Please decipher it and answer the subject of the sentence.

AQDPGSTQRPHD, SQ AQDPGSKSTD EZ GHV PQRAGEAV RFN ZGWND SU GVAHFELWVZ USQ ZVAWQV ASBBWFEARGESF EF GHV PQVZVFAV SU RNMVQZRQERK CVHRMESQ. BSQV TVFVQRKKD, AQDPGSTQRPHD EZ RCSWG ASFZGQWAGEFT RFN RFRKDXEFT PQSGSASKZ GHRG PQVMVFG GHEQN PRQGEVZ SQ GHV PWCKEA UQSB QVRNEFT PQEMRGV BVZZRTVZ. BSNVQF AQDPGSTQRPHD VOEZGZ RG GHV EFGVQZVAGESF SU GHV NEZAEPKEFVZ SU BRGHVBRGEAZ, ASBPWGVQ ZAEVFAV, EFUSQBRGESF ZVAWQEGD, VKVAGQEARK VFTEFVVQEFT, NETEGRK ZETFRK PQSAVZZEFT, PHDZEAZ, RFN SGHVQZ. ASQV ASFAVPGZ QVKRGVN GS EFUSQBRGESF ZVAWQEGD (NRGR ASFUENVFGERKEGD, NRGR EFGVTQEGD, RWGHVFGEARGESF, RFN FSF-QVPWNERGESF) RQV RKZS AVFGQRK GS AQDPGSTQRPHD. PQRAGEARK RPPKEARGESFZ SU AQDPGSTQRPHD EFAKWNV VKVAGQSFEA ASBBVQAV, AHEP-CRZVN PRDBVFG ARQNZ, NETEGRK AWQQVFAEVZ, ASBPWGVQ PRZZYSQNZ, RFN BEKEGRQD ASBBWFEARGESFZ.

Problem 2: Pseudorandomness (25pt)

Let $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a secure PRP (Pseudo-Random Permutation). Consider the family of permutations $E' : \{0,1\}^k \times \{0,1\}^{2n} \to \{0,1\}^{2n}$ defined for all $x, x' \in \{0,1\}^n$ by

$$E'_K(x\|x') = E_K(x)\|E_K(x \oplus x').$$

Show that E' is not a secure PRP.

Problem 3: Proof of security (25pt)

Let $E : \{0,1\}^k \times \{0,1\} \to \{0,1\}$ be a blockcipher. The two-fold cascade of E is the blockcipher $E^{(2)} : \{0,1\}^{2k} \times \{0,1\} \to \{0,1\}$ defined by

$$E^{(2)}_{K_1,K_2}(x) = E_{K_1}(E_{K_2}(x))$$

for all $K_1, K_2 \in \{0,1\}^k$ and all $x \in \{0,1\}$. Prove that if E is a secure PRP then so is $E^{(2)}$.

Problem 4: Hash function (25pt)

A hash function is said to have second preimage resistance if given an input x and its hash $h(x)$, it is computationally infeasible to find another input y (where $y \neq x$) such that $h(y) = h(x)$. Prove that if a hash function h is collision resistant, h is second preimage resistant. Also prove that the inverse is not always true.