Principles of Information Security

Question set for quiz

January 28, 2019

1. Consider an improved version of the Vigenere cipher, where instead of using multiple shift ciphers, multiple mono-alphabetic substitution ciphers are used. That is, the key consists of t random permutations of the alphabet, and the plaintext characters in positions $i, t+i, 2t+i$, and so on are encrypted using the i^{th} permutation. Show how to break this version of the cipher.

2. In an attempt to prevent Kasiski's attack on the Vigenere cipher, the following modification has been proposed. Given the period t of the cipher, the plaintext is broken up into blocks of size t. Within each block, the Vigenere cipher works by encrypting the i^{th} character with the i^{th} key (using a basic cipher). Letting the key be $k_1, ..., k_t$, this means the i^{th} character in each block is encrypted by adding k_i to it, modulo 26. The proposed modification is to encrypt the i^{th} character in the j^{th} block by adding $k_i + j$ modulo 26. (a) Show that decryption can be carried out. (b) Describe the effect of the above modification on Kasiski's attack.

3. Show that the shift, substitution, and Vigenere ciphers are all trivial to break using a known-plaintext attack. (Assuming normal English text is being encrypted in each case.) How much known plaintext is needed to completely recover the key for each of the ciphers (without resorting to any statistics)?

4. Show that the shift, substitution, and Vigenere ciphers are all trivial to break using a chosen-plaintext attack. How much plaintext must be encrypted in order for the adversary to completely recover the key? Compare to the previous question.

5. Prove or refute: For every encryption scheme that is perfectly secret it holds that for every distribution over the message space $\mathcal{M}$, every $m, m' \in \mathcal{M}$, and every $c \in \mathcal{C}$:

$$Pr[\mathcal{M} = m | \mathcal{C} = c] = Pr[\mathcal{M} = m' | \mathcal{C} = c]$$

6. When using the one-time pad (Vernam's cipher) with the key $k = 0^l$, it follows that $Enc_k(m) = k \bigoplus m = m$ and the message is effectively sent in the clear! It has therefore been suggested to improve the one-time pad by only encrypting with a key $k \neq 0^l$ (i.e., to have Gen choose k uniformly at random from the set of non-zero keys of length l). Is this an improvement? In particular, is it still perfectly secret? Prove your answer. If your answer is positive, explain why the one-time pad is not described in this way. If your answer is negative, reconcile this fact with the fact that encrypting with 0^l doesnt change the plaintext.

7. Prove or refute: Every encryption scheme for which the size of the key space equals the size of the message space, and for which the key is chosen uniformly from the key space, is perfectly secret.

8. Consider the following definition of perfect secrecy for the encryption of two messages. An encryption scheme (Gen, Enc, Dec) over a message space $\mathcal{M}$ is perfectly-secret for two messages if for all distributions over $\mathcal{M}$, all $m, m' \in \mathcal{M}$, and all $c, c' \in \mathcal{C}$ with $Pr[C = c \wedge C' = c] > 0$:
$Pr[M = m \wedge M' = m' | C = c \wedge C' = c'] = Pr[M = m \wedge M' = m']$, where m and m' are sampled independently from the same distribution over $\mathcal{M}$. Prove that no encryption scheme satisfies this definition.

9. Consider the following definition of perfect secrecy for the encryption of two messages. An encryption scheme (Gen, Enc, Dec) over a message space $\mathcal{M}$ is perfectly-secret for two messages if for all distributions over $\mathcal{M}$, all $m, m' \in \mathcal{M}$, and all $c, c' \in \mathcal{C}$ with $c \neq c'$ and $Pr[C = c \wedge C' = c] > 0$:
$Pr[M = m \wedge M' = m' | C = c \wedge C' = c'] = Pr[M = m \wedge M' = m' | M \neq M']$, where m and m' are sampled independently from the same distribution over $\mathcal{M}$. Show an encryption scheme that provably satisfies this definition. How long are the keys compared to the length of a message?

10. Say we require only that an encryption scheme (Gen, Enc, Dec) over a message space $\mathcal{M}$ satisfy the following: for all $m \in \mathcal{M}$, the probability that $Dec_k(Enc_k(m)) = m$ is at least 2^{-t} . (This probability is taken over choice of k as well as any randomness that may be used during encryption or decryption.) Show that perfect secrecy can be achieved with $|\mathcal{K}| < |\mathcal{M}|$ where $\mathcal{K}$ is key space.

11. Let $\in < 1$ be a constant and say we only require that for any distribution over $\mathcal{M}$, any $m \in \mathcal{M}$, and any $c \in \mathcal{C}$

$$|Pr[M = m | C = c] - Pr[M = m]| < \in.$$

Prove a lower bound on the size of the key space $\mathcal{K}$ relative to $\mathcal{M}$ for any encryption scheme that meets this definition.

12. (a) A private-key encryption scheme Π =(Gen, Enc, Dec) has indistinguishable encryptions in the presence of an eavesdropper if for all probabilistic polynomial-time adversaries $\mathcal{A}$ there exists a negligible function negl such that $Pr[PrivK^{eav}_{\mathcal{A},\Pi}(n) = 1] \leq \frac{1}{2} + negl(n)$, where the probability is taken over the random coins used by $\mathcal{A}$, as well as the random coins used in the experiment.

(b) A private-key encryption scheme Π =(Gen, Enc, Dec) has indistinguishable encryptions in the presence of an eavesdropper if for all probabilistic polynomial-time adversaries $\mathcal{A}$ there exists a negligible function negl such that $|Pr[output(PrivK^{eav}_{\mathcal{A},\Pi}(n, 0)) = 1] - Pr[output(PrivK^{eav}_{\mathcal{A},\Pi}(n, 1)) = 1]| \leq negl(n)$.

Prove the equivalence between (a) and (b)

13. Let G be a pseudorandom generator where $|G(s)| \geq 2|s|$
(a) Define $G'(s) = G(s0^{|s|})$. Is G' necessarily a pseudorandom generator?
(b) Define $G'(s) = G(s_1 ... s_{n/2})$, where $s = s_1 ..... s_n$. Is G' necessarily a pseudorandom generator?

14. Let (Gen, Enc, Dec) be an encryption scheme defined as follows:
(a) Gen outputs a key k for a pseudorandom permutation F.
(b) Upon input $m \in \{0,1\}^{n/2}$ and key k, algorithm Enc chooses a random string $r \leftarrow \{0,1\}^{n/2}$ of length $n/2$ and computes $c = F_k(r||m)$.
Show how to decrypt, and prove that this scheme is CPA-secure.

15. Let Π_1 =(Gen1, Enc1, Dec1) and Π_2 = (Gen2, Enc2, Dec2) be two encryption schemes for which it is known that at least one is CPA-secure. The problem is that you dont know which one is CPA-secure and which one may not be. Show how to construct an encryption scheme Π that is guaranteed to be CPA-secure as long as at least one of Π_1 or Π_2 is CPA-secure. Provide a proof of your answer.

16. Explain discrete logarithm problem in short and calculate 34^{68} mod 137 with details.

17. Prove that finding most significant bit of the exponent is a hard-core predicate of discrete logarithm problem.

18. Build a pseudorandom generator assuming discrete logarithm problem is hard and msb is hard-core predicate.