Name: ____________

ID: ____________

Grade:____________

03/22/2011

Classic cipher, Perfectly-Secret Encryption
Private-Key Encryption, Pseudorandomness

1.4 Show that the shift, Mono-Alphabetic sub., and Vigenère ciphers are all trivial to break using a known-plaintext attack. How much known plaintext (how many characters) is needed to completely recover the key for each of the ciphers? (show how to break the cipher)

Shift:

Mono-Alphabetic sub.:

Vigenère:

■

1.5 Show that the shift, Mono-Alphabetic sub., and Vigenère ciphers are all trivial to break using a chosen-plaintext attack. How much plaintext (how many characters) must be encrypted to completely recover the key? (show your chosen plaintext)

Shift:

Mono-Alphabetic sub.:

Vigenère:

■

1.6 What is the index of coincidence of your name in Pinyin (without blank space and ignoring case)?

Name:
Letters and their corresponding probabilities in your name:

IC = ∎

2.1 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 $c \in \mathcal{C}$:

$$\Pr[M = m | C = c] = \Pr[M = m' | C = c].$$

∎

2.2 Study conditions under which the shift, mono-alphabetic sub., and Vigenère cipher ciphers are perfectly secret:

- (a) Prove that if only a single character is encrypted, then the shift cipher is perfectly secret.
- (b) What is the largest plaintext space M you can find for which the mono-alphabetic sub. cipher provides perfect secrecy?
- (c) Show how to use the Vigenère cipher to encrypt any word of length t so that perfect secrecy is obtained (note: you can choose the length of the key). Prove your answer.

(a) Shift:

(b) Mono-alphabetic sub.:

(c) Vigenère cipher.:

■

3.1 The best algorithm known today for finding the prime factors of an n-bit number runs in time $2^c \cdot n^{\frac{1}{3}(\log n)^{\frac{1}{3}}}$. Assuming 4Ghz computers and $c = 1$, estimate the size of numbers that cannot be factored for the next 100 years.

(Do not only give the value of n, show the process of solving it.)

■

3.2 Prove that Definition 1 (see handout '3privatekey.pdf') cannot be satisfied if Π can encrypt arbitrary-length messages and the adversary is not restricted to output equal-length messages in experiment $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n)$.

(Show what the adversary would output, and the probability the experiment will success.)

■

3.3 Assuming the existence of a pseudorandom function, prove that there exists an encryption scheme that has indistinguishable multiple encryptions in the presence of an eavesdropper (i.e. Definition 8), but is not CPA-secure (i.e. Definition 10). (see handout '3privatekey.pdf')

Hint: You will need to use the fact that in a CPA the adversary can choose its queries to the encryption oracle adaptively (i.e., new query may be constructed from previous queries).

∎

3.4 Present a construction of a variable output-length pseudorandom generator from any pseudorandom function. Prove that your construction satisfies Definition 7 (see handout '3privatekey.pdf').

∎

3.5 Present formulas for decryption of all the different modes of operation for encryption. For which modes can decryption be parallelized?

ECB:

CBC:

OFB:

CRT:

∎

3.6 Show that the CBC, OFB and CRT modes do not yield CCA-secure encryption schemes (regardless of F).

CBC:

OFB:

CRT:

∎