Chap 2.

2. 공격자가 메시지 M과 그것에 대응되는 암호문 C를 알고 있고, 암호화 알고리즘이 결정적 알고리즘일 때 원격에 있는 두 사용자가 C를 다시 교환하게 되면 공격자가 어떤 메시지를 교환하였는지 알게 된다. 따라서 암호화 알고리즘은 확률적 알고리즘이 되는 것이 안전성에 바람직하다. 그런데 공개키 암호알고리즘에서는 이것이 더욱 더 필요하다. 그 이유를 설명하시오.

A. 공개키 암호 알고리즘에서 확률적 알고리즘이 더욱 더 필요한 이유는, 키가 공개된 상태에서 평문 M과 그것에 대응하는 암호문 C를 알게 된다면, 이를 이용하여 공개된 키로 암호를 해독할 수 있게 되기 때문이다. 공개키 암호 알고리즘은 공개키로 암호화 한 후에 비밀키로 복호화 하여 메시지를 확인하기 때문에, 키 두 개를 사용하는것에 큰 메리트가 있는 암호화 기술인데, 만일 공개키만으로도 평문을 유추할 수 있게 되면 공개키 암호 알고리즘을 사용하는 의미가 사라지기도 하기 때문이다.

6. 영문 텍스트를 암호화하는 방법으로 매핑하는 테이블을 이용한다고 가정하자. 즉, 26개의 영문 문자를 각각 다른 영문 문자로 매핑하는 테이블(A → C, B → N, ..., Z → A)을 이용하는 것을 말한다. 다음 각각에 대해 답변하시오.

   ① 가능한 키의 개수는?

   ② 이와 같은 방식으로 암호화하였을 때 문제점을 한 가지 설명하시오. (키의 개수나 보관과 관련된 문제는 아니며, 공백, 마침표, 특수문자 등의 암호는 무시하고 암호문을 통해 노출되는 정보가 무엇인지 생각해보시오)

A - 1. 영문자 26개를 각각 다른 영문자 26개로 매핑하여 사용하는 것 이기 때문에 26!개의 매핑 경우가 나온다. 따라서 이 매핑 경우마다 키를 할당한다면 26!개의 키가 사용 가능하다.
A - 2. 이런 암호화 방식은 교체연산을 여러번 진행해야 안전성을 높일 수 있기 때문에, 동일한 과정을 여러번 반복하지 않고 한 번만 반복한다면 쉽게 암호를 해독할 수 있게 된다. 예를 들여 알파벳에서 가장 많이 사용되는 알파벳은 e라는 통계 자료가 있기 때문에 이를 토대로 경우의수를 따져가며 한글자씩 알아낼 수 있게 된다.

7. HTTPS 프로토콜로 접속이 가능한 웹 사이트에 접속하여 해당 사이트의 인증서 정보를 추출하여 발급한 인증기관, 공개키의 종류, 공개키의 길이와 같은 중요 정보를 제시하시오.

A. openssl을 사용하여 cmd에서 openssl s_client -connect google.com:443 을 입력하여 인증서를 추출했다.

Server public key is 2048 bit
이 부분에서 공개키의 길이가 2048 bit인것을 알 수 있다.

depth=2 C = US, O = Google Trust Services LLC, CN = GTS Root R1
이 부분에서 인증서의 발급 기관이 GTS Root R1인것을 알 수 있다.

Peer signing digest: SHA256
이 부분에서 공개키의 종류는 SHA256인 것을 알 수 있다.