품질 연계지표 평가방법을 사용한 암호화 모듈 실무현장 적용체계 연구★

노시춘* · 나상엽**

본 연구에서 제안하는 암호화 모듈 품질평가 체계는 ISO/IEC 9000 품질체계를 참조하여 Quality, Quality Factor, Quality Subfactor, Metric로 계층화된다. 암호화 알고리즘 실무적용 프로세스는 암호화 알고리즘 장단점 진단을 기초로 하여 암호화자산 평가, 알고리즘선택 포인트 분석, 품질 항목(quality factor) 도출, 제약조건도출, 암호모듈 품질평가체계 설계 등 5개단계로 설정한다. 이 5개 단계는 현장중심의 암호화 작업사례를 진단하여 업무에서 가장 필수적으로 수행되어야 할 작업순서를 도출한 것 이다. 2-Factor간 연계지표는 암호화 모듈의 품질항목(quality factor)을 발굴하고 이 품질 항목을 확보하는 환경인 암호화 작업의 제약조건 두가지 영역이다. 본 연구는 암호화 모듈 실무현장 적용체계를 하나의 표준화 모델로 제시한다. 우리는 정보기술 환경의 급속한 변화에 부응하여 암호화 알고리즘 개발과 현장 적용 모델을 다양하게 개발하므로서 암호화의 효율을 기대할 수 있을 것 이다.

A Study of Practical Field Application Cryptographic Module through Evaluation Derived by Connection Indicators

SiChoon Noh* · SangYeob Na**

Abstract

In this study, we propose a cryptographic module quality evaluation system referenced by ISO/IEC 9000 quality system with Quality, Quality Factor, Quality Subfactor, Metric. Practical application process encryption algorithm based on the encryption algorithm to encrypt the pros and cons valuation of diagnosis, point selection algorithm, analysis, and quality items(quality factor), eliciting constraints derived, such as the cryptographic module design quality evaluation system is set to step 5. The five steps are examples of field-based diagnostic tool for cryptographic operations, the most essential work to be done in order to derive one will work. 2-Factor encryption module for connection between indicator items(quality factor) to identify and ensure the quality of the item the constraints of the environment are two kinds of cryptographic operations. This study is an encryption module and a practical field application system, it presents the standardized model. We have to meet the rapid changes in information technology. The environment, development and the encryption algorithm applied to model a wide variety of on-site development encryption will be able to expect the efficiency.

keywords : Practical ; Field Application; Cryptographic Module; Evaluation ; Connection Indicators

접수일(2014년 5월 30일), 수정일(1차: 2014년 6월 16일), 게재확정일(2014년 6월 17일)

★ 본 연구는 2014년 남서울대학교 연구비 지원으로 이루어졌음.

* 남서울대학교 컴퓨터학과

** 남서울대학교 컴퓨터학과 (교신저자)

1. 서 론

암호화 기술은 전송되거나 저장된 평문의 의미를 제3자가 알수 없도록 평문을 의미를 알 수 없는 형태인 암호문으로 전환하는 암호화와 암호화된 암호문을 다시 원래 정보 형태로 복구시키는 기술인 복호화 기술로 구분된다. 암호화 알고리즘은 방식별로 모두 특성과 장단점을 가지고 있다. 따라서 실무현장에서는 어떤 종류의 알고리즘이 업무에 유리한지 여부를 잘 판단해야 한다. 암호화 알고리즘에서는 암호화의 비밀성을 높이기 위해 키(Key)를 사용한다. 암호화는 보안에 대처하는 가장 강력한 수단이자 필수적 방법이지만 이 방법을 실제로 업무에 적용하기 위한 효율적인 절차와 방법론에 대해서는 제시된 안이 부족하여 실무에서 어려움이 많다. 그 이유는 암호화 관련 연구는 알고리즘 연구에 집중되고 있어 실제 암호화 절차와 알고리즘 선택 포인트 등 현장 적용 방법론을 연구한 사례가 없다. 본 연구는 이같은 상황을 고려하여 암호화 모듈 현장적용 체계를 설계하여 작업순서를 도출하고 암호화 알고리즘 선택 포인트를 도출하며 암호모듈 품질평가방법을 개발하여 제시한다. 이 연구는 현장중심의 사례 중심으로 필수적 수행 작업을 도출하며 이 모델을 통하여 업무현장에서 암호화 적용 효율을 높이기 위한 방법을 제시하기 위한 것이다. 논문 기술순서는 암호화 알고리즘 장단점 진단, 암호화 모듈 현장 적용체계 설계, 암호화모듈 품질의 2-Factor간 연계 평가, 결론의 순서이다.

2. 암호화 알고리즘 장단점 진단

2.1 공개키 방식

공개키 방식은 암호화와 동시에 인증 서비스(Authentication)를 제공 하는 디지털 서명이 가능 하다. 안전성과 편의성이 대폭 개선되었고, 공개키 암호 방식은 지수함수의 역인 이산대수의 해를 구하는 어려움 때문에 암호 해독 노력이 크다. 그러나 이 방식은 연산에 소요되는 계산량과 수행시간이 암호강도와 비례하여 요구된다. 공개키 방식의 장점은 동시에 인증서비스를 제공하는 디지털 서명이 가능하다. 지수함수의 역인 이산대수의 해를 구하는 어려움 때문에 암호 해독이 어렵다. 키 관리가 용이하고 완벽한 인증이 가능하다. 공개키 방식의 단점은 연산 소요 계산량과 수행시간이 암호강도와 비례하며 연산에 소요되는 계산량과 수행시간이 크게 요구된다[1][2][4].

2.2 대칭키 방식

비밀키, 대칭키는 알고리즘이 상대적으로 간단하므로 속도가 월등히 빠르고, 소프트웨어로 구성 시 파일의 크기가 작으며, 하드웨어로 구현하는 경우 회로가 간단하다. 키가 노출되면 모든 정보가 침입자에 의해 노출되는 문제점과 키 분배의 문제가 있다. 대칭키는 알고리즘 장점은 알고리즘 이 상대적으로 간단하므로 속도가 빠르다. 소프트웨어로 구성시 파일의 크기가 작으며, 하드웨어로 구현하는 경우 회로가 간단하다. 대칭키는 알고리 즘 단점은 쉽게 깨어지고, 완벽한 인증이 곤란 하다. 불특정 다수간 통신 시 키 생성과 분배에 어려움이 따른다. <표 1>은 대칭 키와 공개키 암호화 알고리즘 장단점 진단이다[1][2][3].

<표 1> 암호화 알고리즘 장단점 진단

구분	대칭키 방식	공개키 방식
장 점	-알고리즘이 상대적으로 간단하므로 속도가 빠르다 - 소프트웨어로 구성시 파일의 크기가 작으며, 하드웨어로 구현하는 경우 회로가 간단 -구현이 쉽고 속도가 빠르다 -여러가지 변형이 가능	-동시에 인증 서비스를 제공하는 디지털 서명 가능 -지수 함수의 역인 이산대수의 해를 구하는 어려움 때문에 암호 해독이 어렵다. -키 관리가 용이 -완벽한 인증이 가능
단 점	-쉽게 깨어지고, 완벽한 인증이 곤란 -불특정 다수간에 통신을 할 때 키의 생성과 분배에 어려움 -키가 노출되면 모든 정보가 침입자에 의해 노출되는 문제점 -키의 분배 문제	-연산 소요 계산량과 수행시간 이 암호강도와 비례 -연산에 소용되는 계산량 과 수행 시간이 엄청나게 요구됨 -양자 컴퓨터가 본격적 으로 실용화되면 RSA 알고리즘은 더 이상 사용 되기가 어려움

3. 암호화모듈 현장적용 체계 설계

3.1 알고리즘 실무적용 프로세스

암호화 알고리즘 장단점 진단을 기초로 하여 본 연구에서 제시하는 암호화모듈 현장적용 순서는 암호화 자산 평가, 알고리즘선택 포인트 분석, 품질 항목(quality factor) 도출, 제약조건도출, 암호모듈품질평가체계설계 등 5개단계로 설정한다. 5개 단계는 현장 중심의 사례를 진단하여 가장 필수적으로 수행되어야 할 작업순서를 정한 것으로서 구성은 다음 <표 2>와 같다.

<표 2> 알고리즘 실무 적용 프로세스

절차	암호화자산 가치평가	알고리즘선택 포인트 분석	품질항목 (quality factor) 도출	제약조건 도출	암호모듈품질평가체계 설계
구성 항목	대상콘텐츠, 평가가치계량화	공개키, 대칭키	5개항목 품질항목	5개항목 제약조건	4개단계품질평가절차

3.2 실무적용 5개 프로세스 내용

3.2.1 알고리즘 선택 포인트 분석

알고리즘 선택 포인트 분석은 알고리즘을 적용할 업무와 자산의 성격에 어느 알고리즘이 적합한지를 선태해주는 포인트이다. 본 연구에서 조사한 선택포인트는 아래와 같이 6개 항목 대칭키 선택 포인트와 6개 항목 공개키 선택 포인트로 조사 되었고 종합적으로는 <표 3> 알고리즘 선택 포인트로 나타난다[3][4].

<표 3> 알고리즘 선택 포인트

구 분	비밀키 방식	공개키 방식
키의 상호관계	비밀키 = 공개키	비밀키 공개키
암호화 키	비밀키	수신측 공개키
복호화 키	비밀키	수신측 사설키
암호알고리즘	DES, SEED, AES	RSA, Diffie Hellman
비밀키 전송	필요	불필요
안전한 인증	곤란	용이
연산 소요계산량	암호강도에 비례	암호강도에 비례하여요구
암호 수행속도	상대적으로 빠르다	상대적 장시간
키의 크기	작다	상대적으로 크다
키의 사전 분배	반드시 필요	불 필요
암호,복호화 키	동일	상이
암호화 대상 규모	소수	다수
경제성	상대적으로 높다	상대적으로 낮다
전자서명	상대적으로 복잡	상대적으로 간단

3.2.2 암호화 모듈 품질항목(quality factor)

① 암호화 적용 프로세스 간편성 : 암호화 적용 대상 콘텐츠는 정보 콘텐츠와 문화 콘텐츠로 나눌 수 있고, 콘텐츠 가공, 제작, 저장기술에 적용된 디지털 기술의 유무에 따라 디지털콘텐츠와 일반 콘텐츠로 나눌 수 있으며 디지털콘텐츠는 유통경로에 따라 온라인 콘텐츠와 오프라인 콘텐츠로 구분된다. 암호 프로그램의 개발 또는 도입 시 암호화 가능한 데이터 및 적용 업무 DB암호화 솔루션으로 암호화 구축이 가능한 업무 및 데이터 종류는 대체적으로 다음과 같다. 적용가능 업무는 고객DB(개인정보, 본인확인용 스캔 문서), 인사DB(개인정보, 고과/연봉 정보), 기술DB(도면, 기술 문서), 기타 DB(CCTV 영상)이다[5][6].

<표 4> 암호화대상 콘텐츠의 분류

구분		정보콘텐츠	문화콘텐츠	교육콘텐츠
디지털콘텐츠	온라인콘텐츠	웹페이지, 전자메일 등의 형태로 유통되는 교육, 보건, 산업 등 각종 정보콘텐츠, DB 콘텐츠 등	MP3 음악파일, 전자책, 사진, 그래픽, 온라인용으로 제작 및 편집된 방송 프로그램 등의 영상물 등	원격 강의, 사이버 강의
	오프라인콘텐츠	디지털로 작성되었으나 온라인에서 유통되지 않는 각종 정보 콘텐츠	디지털 영화, 디지털 애니메이션, DVD, CD-ROM 타이틀, 음반CD 등	교육용 타이틀 및 S/W

<표 5> 암호화 적용 프로세스 간편성 평가표

구분	간편성 평가				
간편성 등급	VL	L	M	H	VH
지수범위	1-20	21-40	41-60	61-80	81-100

② 암호화 강도 수준 : 암호강도(Strength of Cipher)는 암호화 알고리즘을 알고 있는 암호 공격자가 키 혹은 평문을 알아내고자 했을 때의 노력의 정

도를 의미한다. 암호강도가 클수록 그 암호계는 안전한 암호계가 된다. 알고리즘이 공개 된 상태에서 키마저 알려진다면 누구나 쉽게 평문을 알아낼 수 있다. 암호 강도의 정도를 나타내기 위해 사용되는 평가 지표(indicator)가 강도 지표이다. 대표적 강도 지표로 정보이론적인 지표인 암호문으로부터 평문이나 키를 유추해 내기 어려운 정도인 불확정성과, 이와 관련되어 평문이나 키를 유추해 내기 위해 필요한 최소한의 암호문의 길이를 나타내는 판별 거리(Utility Distance)가 있다. 암호공격에 소요되는 계산 횟수를 의미 하는 웍 팩터(Work Factor)는 키를 알지못한 공격자가 모든 가능한 키를 만들어 암호 알고리즘을 수행시킬 때 평문을 찾아낼 수 있는 평균적인 횟수이다[7][8].

③ 시스템 부하수준 : 암·복호에 의해 발생하는 시스템의 부하(load)는 거의 CPU 사이클에 의존 한다. 최근의 병렬처리 시스템 구조는 수십개 4GHz 이상의 Clock CPU가 클러스터링 구조로 장착되는 서버들이 대부분이다. 4GHz로 동작하는 20개의 CPU를 가진 서버를 가정하면 사용가능한 총 CPU 사이클은 80GHz/초당이다. 반면에 Appliance에 통상 장착 되는 CPU들은 이보다 낮은 2GHz 대의 CPU가 4개 정도 장착된다. 이때 가용 사이클은 약 8GHz 정도이다. DB 자체가 암·복 호 부하가 없도록 설계되는 방법이 필요 하며 암호화된 데이터만 가지고는 색인검색이 불가능해지기 때문에 Full Table Scan이 발생 되므로 결과적으로 암·복호화는 이전에 없던 부하를 발생시킨다[9].

④ 성능과 암호화 기능 간 상충(trade off) : 보안체크와 시스템 성능(performance)간에는 상호 같은 성능으로 양립할 수 없는 성질, 즉 상충(trade off)이 발생한다. 정보에 대한 접근 제어와 감사를 실시하고 이를 저장할 때에는 암호화하여 저장한다. 이때 문제는 우선순위의 문제 뿐아니라 시스템 부하로 양자택일 문제가 발생할 수 있다. 암호화는 응답시간 증가 부담 을 동반할 수 있다. 즉, 투자비 지출계획에 의한 도입 순서의 문제가 될 수 있다. 이때 법규만 충족하기 위해 '중요한 우선순위에 의한 정보 레벨을 설정해야 한다. 정보종류에 따라 암호화와 데이터 접근제어를 적절히 배치해야 한다[10][11].

⑤ 암호화 인덱스에 의한 색인검색 : 메타데이터는 통신 네트워크의 형상(topology), 장애나 운용상태, 프로세스나 자원에 관한 정보이다. 어떤 노드에서 데이터베이스를 이용하는 경우, 먼저 메타데이터를 액세스하여 시스템 내에 있는 데이터베이스의 종류, 이용조건, 사용방법 등에 관한 정보를 조사 후 원하는 데이터베이스를 액세스한다. 어느 경우도 메타 데이터는 동적으로 변화한다. 메타 데이터에 대한 다수 복제를 원활하게 또한 정확하게 갱신하기 위해 동시실행 제어가 필요하다. 암호화된 인덱스를 통한 색인 검색 기술은 까다롭고 제공 되어야하는 몇 가지 특별한 기능을 필요로 한다[12],

<표 6> 암호화모듈 품질항목

Factors	Sub-Factors	Metrics	Score	Weighted Score	Final Score
프로세스 간편성	5	%	1-100	0.1-0.9	
암호화 강도수준	4	%	1-100	0.1-0.9	
시스템 부하수준	3	%	1-100	0.1-0.9	
성능과 암호화 기능 간 상충	4	%	1-100	0.1-0.9	
인덱스에 의한 색인검색	4	%	1-100	0.1-0.9	
소계	20	%	1-100	0.1-0.9	

3.2.3 암호화모듈 제약조건 도출

① 애플리케이션 영향 : 암호화로 인한 기존 애플리케이션의 운영에 어떤 영향이 있을 것 인지를 사전에 면밀히 분석 한다. 정기적인 월말 작업이 있다면 이 기간을 포함하여 약 1주간 모니터링하고 DB 서버에 요청하는 쿼리 문장을 분석 영향을 줄 수 있는 문제 쿼리를 찾아낸다.

② 업무전환 방식 : 암호화 방식은 크게 API 방식, Appliance 방식, Plug-In 방식으로 세가지 형태이며 API 방식은 AP 서버에 암호화 모듭을 설치하는 방식이다, API 방식의 제품을 사용하기 위해서는 API 기능이 연결되는 애플리케이션을 수정해주어야 한다. 이때 암.복호기능 수행에 따른 시스템 부하는 AP 서버에 발생하게 된다.

③ 업무규정 충족 : 암호화의 대상 데이터량(volume)의 증가는 곧 DB 처리 응답시간과 산출량의

성능저하와 직결되므로 DB운영성을 고려해야 한다. DB 처리 성능 저하와 DB제약 사항을 고려하여 암호화 대상 업무와 암호화방법론에 대한 적절하고 효율적인 암호화 기준 정립이 필요 하다.

④ 자원 환경 : 암호화 작업에 필요한 여분의 Temporary Disk 공간은 있는지, 기타 DB의 환경변수들은 적절한 지, 필요한 패키지나 패치 레벨 등이 적절히 설치되어 있는지 환경의 준비 가 요구된다. 암호화 전환 작업은 서버성능을 고려하여 비 업무시간대일 경우 가능한 한 Parallel 처리로 짧은 시간내에 마치도록 하여 이 작업동안 서비스 계속 무중단 구축의 효과를 실천한다.

⑤ 테스트와 검증조건 : 암호화 전환작업이 완료되면 데이터가 정확히 변환 되었는지 정합성 체크를 실시한다. 애플리케이션을 수행하여 문제가 있는지 성능저하는 어느 정도인지 확인한다. 암호화는 구축하고 나면 되돌리기 어려워 처음 구축 시 실제 환경 에서 테스트한다. 테스트 모듈은 실제 환경에서 주기적으로 암호 프로그램 등록, 변경 및 운영에 대한 감사 및 확인을 실시한다.

<표 7> 암호화모듈 제약조건

Factor	Sub-Factors	Metrics	Score	Weighted Score	Final Score
애플리케이션 영향	3	%	1-100	0.1-0.9	
업무전환 방식	4	%	1-100	0.1-0.9	
업무규정충족	3	%	1-100	0.1-0.9	
자원 환경	3	%	1-100	0.1-0.9	
테스트와 검증	4	%	1-100	0.1-0.9	
소계	17	%	1-100	0.1-0.9	

4. 품질지표 평가방법

평가지표의 동일 분류내 척도를 산출한 후 각 지표의 품질 측정값 연계지표를 작성한다. 연계지표는 암호화 모듈의 품질항목(quality factor)을 발굴하고 이 품질 항목을 확보하는 환경인 암호화 작업의 제약조건 두가지 영역이다. ISO/IEC 9000의 정의에 의하면 품질은 사용 시 사용자 요구사항을 만족시키는 제품이나 서비스 특성을 종합한 개념이다. 품질 모델(quality model)은 품질 속성을 분류 하고 정의하여 누구나 인정할 수 있는 품질 측정기준을 정의한다. ISO/IEC 9000 품질 체계는 품질(quality), 품질항목(quality factor), 세부항목(quality subfactor), 측정기준(metric)으로 계층화 된다. 평가지표의 동일 분류내 척도를 산출한 후 각 지표의 중요도를 산출하여 가중값을 부여한다.

<표 8> Rating Matrics

Factor	애플리케이션 영향	업무전환 방식	업무규정 충족	자원 환경	테스트와 검증	Total
프로세스 간편성						%,
암호화 강도						%,
시스템 부하수준						%,
성능과 암호화 기능 간 상충						%,
인덱스에 의한 색인검색						%,
Total						%,

5. 결 론

암호화품질 모델은 품질속성을 분류하고 정의하여 누구나 인정할 수 있는 품질모델 도입 시 시스템 품질 정식화(formalization)가 가능하다. 측정 체크리스트는 품질 파라메터별 측정기준 을 점검방법에 따라 점검한다. 본 연구에서 제안하는 암호화 모듈 품질체계는 ISO/IEC 9000 품질체계를 참조하여 Quality, Quality Factor, Quality Subfactor, Metric로 계층화 한다. 알고리즘 실무 적용 프로세스는 암호화 알고리즘 장단점 진단을 기초로 하여 본 연구 에서 제시하는 암호화 모듈 현장적용 순서는 암호화자산 평가, 알고리즘 선택 포인트 분석, 품질항목(quality factor) 도출, 제약 조건도출, 품질 만족도 평가 등 5개단계로 설정 한다. 5개단계는 현장중심 사례를 진단하여 가장 필수적으로 수행되어야 할 작업순서를 도출한다. 평가

지표의 동일 분류 내 척도를 산출한 후 각 지표의 중요도를 평가하여 중요도별로 가중값을 부여한다. 본 연구가 암호화 적용을 준비하고 있는 각종 인트라넷 시스템의 현장실무에 참고되기를 기대한다.

참고문헌

[1] R. L. Rivest, A. Shamir, L. Adleman, "A Method for Obtaining Digital. Signatures and Public-Key Cryptosystems", Communications of the ACM vol. 21. pp 8~10, 1978

[2] Imai H., Hanaoka G., Shikata J., Otsuka A., Nascimento A.C. 2002. Cyptography with Information Theoretic Security. Information Theory Workshop, 2002, Proceedings of the IEEE, 20-25 Oct 2002.

[3] Li, S., Zheng, X., 2002. On the Security of an Image Encryption Method. ICIP2002.

[4] Menezes, A. J., P.C. Van Oorschot, S.A. Van Stone. 1996.Handbook of Applied Cryptography. CRC press.

[5] Overbey, J., Traves, W., Wojdylo, J., 2005. On the keyspace of the Hill cipher. Cryptologia, 29(1):59-72.

[6] A. Diffie, M. E. Hellman, ''New directions in cryptography", IEEE Trans. Inf. Theory IT-26, no. 6., pp. 644~654, 1976

[7] Bibhudendra Acharya, Girija Sankar Rath, Sarat Kumar Patra, Saroj Kumar Panigrahy. 2007. Novel Methods of Generating Self-Invertible Matrix for Hill Cipher Algorithm, International Journal of Security, Vol 1, Issue 1, 2007, pp. 14-21.

[8] P.W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring", Proceedings, 35th Annual Symposium on Fundamentals of Computer Science (FOCS), pp. 124~134.. 1994

[9] Tom M. Apostol, "Calculus", Volume 1, Blaisdell Publishing Company, pp 422~423, 1962

[10] Brian S. Thomson, Andrew M. Bruckner, "Elementary Real Analysis Second Edition", CreateSpace, pp 85, 2008

[11]O.Elkeelany, M.M.Matalgah, K.P.Sheikh , M.Thaker, G.Chaudhry, D.Medhi, J.Qaddour, ""Performance Analysis of IPSec Protocol: Encryption and Authentication"", 1164-1168, IEEE 2002

[12] Alan O.Freier, Philip Karlton, Paul C.Kocher, "he SSL Protocol Version 3.0" Internet-Draft, November 1996

[저 자 소 개]

노 시 춘 (SiChoon Noh)

1987년2월 : 고려대학교 경영정보학 석사
2005년2월 : 경기대학교 정보보호기술 박사
2002년11월 : KT 시스템보안부장
2004년 12월 : KT 충청전산국장
2005년3월 ~ 현재 :남서울대학교 컴퓨터학과 교수
IT융합연구소연구위원

email : nsc321@nsu.ac.kr

나 상 엽 (SangYeob Na)

1992년 2월 동국대학교 전자계산학과 (공학사)
1995년 2월 동국대학교대학원 컴퓨터공학과 (공학석사)
2000년 2월 동국대학교대학원 컴퓨터공학과 (공학박사)
1996년 3월 ~ 현재 남서울대학교 컴퓨터학과 교수

email : nsy@nsu.ac.kr