情報保護學會論文誌
第19卷 第4號, 2009. 8

금융부문 암호기술의 안전성 강화를 위한 보안고려사항

김 영 태,[1†] 이 수 미,[2] 노 봉 남[3‡]
[1]전남대학교 정보보호 협동과정, [2]금융보안연구원, [3]전남대학교 시스템보안연구센터

The Considerable Security Issues on the Security Enforcement of Cryptographic Technology in Finance Fields

Young-Tae Kim,[1†] Su-Mi Lee,[2] Bong-Nam Noh[3‡]
[1]Interdisciplinary Program of Information Security, Chonnam National University,
[2]Financial Security Agency,
[3]System Security Research Center, Chonnam National University

요 약

최근까지 암호기술에 대해 알려진 공격이나 안전성 저하현상에 의해 국내외 주요기관들은 권장되는 암호기술의 종류, 사용기간, 안전성 파라미터 등을 명확하게 명시하고 있다. 이에 따라 국내 금융권에서도 일부 암호기술을 교체하기 위한 작업이 이루어져야 할 것이다. 본 논문에서는 금융권에서 시급히 이루어져야하는 금융권 암호기술 적용 현황 파악 및 취약 암호기술 선별 등 선행작업과 금융권 암호기술관리 방안에 대해 살펴보고, 향후 암호기술의 안전성에 대한 급격한 변화에도 금융시스템의 신뢰도를 유지할 수 있도록 중장기적인 관점에서의 암호기술 관리방안에 대해 제시한다.

ABSTRACT

By known attacks against cryptographic technology and decline of security, internal and external major institutions have defined their recommendations in kinds, expiration, safe parameters of cryptographic technology and so on. Internal financial fields will change some cryptographic technology to follow these recommendations. To keep strong security of financial systems against sudden security changes of cryptographic technology, this article finds pre-steps : status of applied cryptographic technology, selection of vulnerable cryptographic technology. And plans for management of cryptographic technology in financial fields will be proposed.

Keywords: cryptographic technology, financial fields

I. 서 론

주요 금융정보의 보호와 금융거래에 대한 인증을 위해 전자금융거래에 사용되는 암호기술은 모바일 뱅킹, 인터넷 전자금융, 텔레뱅킹, 금융자동화기기 거래 등 다양한 금융서비스로 활용되고 있으며, 2Key-Triple DES, RC4, 1024비트 RSA, SHA-1 등이 주요 암호기술로 적용되고 있다. 금융권에 적용된 일부 암호기술은 암호해독 기술의 향상 등을 이유로 충분한 안전성을 확보하기 어렵다는 견해가 이미 암호전문가에 의해 제기된 바 있으며, 미 국립표준기술연구소(NIST)에서는 2010년 이후 미국연방정부기관시스템에서 권장 암호기술로 교체하는 방침[4,5]을 제시하고 있다. 이에 따라 국내에서도 암호 알고리즘, 암호키 길이 등의 교체에 대한 움직임이 일어나고 있다.

접수일(2009년 2월 11일), 수정일(1차: 2009년 5월 7일, 2차: 2009년 6월 12일), 게재확정일(2009년 7월 21일)
† 주저자, ytkim@fsa.or.kr
‡ 교신저자, bbong@jnu.ac.kr

이러한 현상으로 공인인증기관에서 전자서명에 사용되는 1024비트 RSA 암호알고리즘을 2048비트로 향상시키는 방안을 추진하고 있고, 암호모듈 검증기관 또한 SHA-1 등 해쉬함수에 대한 교체를 고려 중에 있다. 따라서 국내 금융시스템에서 이용 중인 암호기술을 세부적으로 분석하여 전자금융서비스 유형별로 암호 알고리즘 종류, 암호키 길이 등 '금융권 암호기술 적용 현황'을 파악하고, 암호기술 교체 시 상호연동성 문제에 수반될 수 있는 영향을 최소화하기 위한 암호기술 교체 방안이 시급히 선행되어야 할 것이다. 이를 바탕으로 향후 암호기술의 급격한 변화에 원활히 대응하기 위해 지속적으로 금융권 암호기술을 분석하고 모니터링을 할 수 있는 체계를 갖추어야 할 것이다.

II. 암호기술의 안전성 평가

2.1 주요기관 및 국제표준의 안전성 평가

NIST, ISO, CRYPTREC, NESSIE 등 주요기관 및 표준에서 인정되는 암호기술 중 암호알고리즘에 대한 블럭암호, 전자서명, 해쉬함수를 규정하는 NIST의 FIPS[1]와 SP[2]에는 블럭암호 AES, 2Key/ 3Key Triple DES 등, 전자서명은 RSA, DSA, ECDSA, 해쉬함수는 SHA-1, SHA-2, 키분배는 Menezes- QU-Vanstone(MQV), Diffie-Hellman(DH)로 규정하고 있다[표 1].

[표 1] FIPS 및 SP에 규정된 암호 알고리즘

규격번호	규정 알고리즘	암호분류
FIPS 197	AES	블록암호
SP 800-67	2-Key/3-Key Triple DES	블록암호
FIPS 185	Skipjack	블록암호
FIPS 186-2	RSA, DSA, ECDSA	전자서명
FIPS 180-2	SHA-1, SHA-2	해쉬함수
SP 800-56	MQV, DH	키분배

해당 주요 지침으로는 미연방정부의 정보보호시스템에 사용되는 암호기술의 안전성을 유지하기 위해, 키 관리에 대한 가이드라인을 SP 800-57 [7]과 SP 800-78 [6]에 제시하였다. SP 800-57에서 변경방침 중 2010년 이후 112비트 2-Key Triple DES, 1,024비트 RSA, 1,024비트 DSA, SHA-1에 대한 사용제한을 권고하고 있고, 미연방정부기관 시설과 정보시스템 등에 접근할 때, 사용되는 암호기술에 대해 기술된 SP 800-78 [표 2]는 해쉬함수 SHA-1, SHA-224, SHA-256 경우 2010년까지 사용을 권장하고 있고, 이후 SHA-224, SHA-256의 사용을 권장하고 있다. 이외에도 카드 인증, 전자서명, 키분배용 암호기술에 사용될 암호 알고리즘과 암호키 길이에 대해 사용기간, 권장 암호알고리즘, 안전성 파라미터들을 명확하게 제시하고 있다.

[표 2] SP 800-78에 기술된 암호 알고리즘 변경 지침

암호키 종류	사용 기간	권장 암호알고리즘 (안전성 파라미터)	
개인 식별키 (공개키 암호)	2010년 까지	RSA (1,024, 2,048, 3,072비트) ECDSA (224비트~283비트)	
	2010년 이후	RSA (2,048, 3,072비트) ECDSA (224비트~283비트)	
PIV카드 인증키 (블록 암호 또는 공개키 암호)	2010년 까지	블록 암호	2-Key Triple DES (112비트) 3-Key Triple DES (168비트) AES (128, 192, 256비트)
		공개키 암호	RSA (1,024, 2,048, 3,072비트) ECDSA (224비트~283비트)
	2010년 이후	블록 암호	3-Key Triple DES (168비트) AES (128, 192, 256비트)
		공개키 암호	RSA (2,048, 3,072비트) ECDSA (224비트~283비트)
전자서명 생성키 (공개키 암호)	2008년 까지	RSA (1,024, 2,048, 3,072비트) ECDSA (224비트~283비트)	
	2008년 이후	RSA (2,048, 3,072비트) ECDSA (224비트~283비트)	
키분배용 키 (공개키 암호)	2008년 까지	RSA (1,024, 2,048, 3,072비트) ECDH / ECC MQV (224비트~283비트)	
	2008년 이후	RSA (1,024, 2,048, 3,072비트) ECDH / ECC MQV (224비트~283비트)	

III. 암호기술에 대한 알려진 공격유형

주요 암호화 방식인 대칭키암호, 공개키암호와 해쉬함수에 대해 학술적으로 알려진 공격유형들을 살펴본다 [표 3].

3.1 대칭키암호

대칭키암호는 블록암호와 스트림암호로 분류되며,

1) FIPS (Federal Information Processing Standard) : 미국연방정부내 시스템에서 채택된 정보기술에 대한 규정
2) SP(Special Publications) : 일반적인 권장기술, 또는 FIPS 부수정보

〔표 3〕 암호알고리즘의 알려진 공격유형

암호유형	종 류	공격 가능성
대칭키 암호	블록암호 (2Key Triple DES, RC2)	키전수공격법보다 적은 계산량으로 비밀키 추정이 가능
	스트림암호 (RC4)	WEP의 이용형태에서 RC4키 공격가능
공개키 암호	RSA	1024비트 합성수가 현실적으로 소인수 분해가능
	DSA/DH	소인수 분해와 동일 계산량을 유지하므로 1024 키길이에 대한 공격 가능성
	ECDSA/ ECDH	160비트 키길이는 RSA 1024비트 키길이와 동일한 안전성을 의미
해쉬 함수	SHA-1	충돌에 의한 공격 가능성
	MD5	실제 충돌 공격에 의한 전자서명 위조사례

블록암호에 대한 공격유형은 숏컷공격법과 브루트포스공격법이 존재한다. 숏컷공격법은 암호알고리즘의 취약점을 이용하여, 암호키를 효율적으로 찾아내는 기법이다. 이러한 숏컷공격으로 인해 SSL에서 사용 중인 64비트 RC2는 전수조사보다 적은 계산량으로 암호키를 탐색할 수 있다는 것이 학술적으로 밝혀졌다.

또한 2Key-Triple DES나 3Key-Triple DES는 암호키 후보를 순차적으로 시험하여 암호키와 평문에 대한 정보를 얻어내는 브루트 포스공격법에 의해 암호키를 해독할 수 있는 가능성이 높은 것으로 알려졌다. 즉 브루트포스 공격법은 2Key-Triple DES와 3Key- Triple DES에 대해 전수조사보다 적은 계산량으로 암호키를 추정 가능하고 〔2,3〕, 2Key-Triple DES의 경우, 공격 가능한 계산량이 현실적으로 해독이 가능한 영역까지 도달하였으며, 3Key-Triple DES의 경우는 2Key-Triple DES 보다 많은 계산량이 요구되어 학술적으로만 해독이 가능한 것으로 판단되고 있다.

3.2 공개키암호

공개키암호로 대표적인 RSA는 그 안전성이 큰 합성수에 대한 소인수분해의 어려움에 근간을 두고, 전자서명이나, 암호화에 이용되고 있다. 하지만 2018년쯤 1,024비트 합성수는 무어의 법칙[3]을 기반으로 현실적으로 소인수분해가 가능하다는 결과가 제시되었으며, 이에 1,024비트 RSA의 안전성을 확보하기 위해서는 2010년까지 사용을 권장하고 있다. 또한 DSA와 DH의 안전성은 이산대수문제의 어려움에 그 근간을 두고 있다. 이산대수문제를 풀기 위한 알고리즘으로는 지수계산법이 있으며, 이 계산량은 소인수분해문제를 풀기위한 알고리즘의 계산량과 동일하다는 평가를 받기 때문에 2010년 시점에 1,024비트 합성수의 소인수분해가 가능하다는 상황에서 DSA와 DH도 재검토가 이루어져야 한다.

3.3 해쉬함수

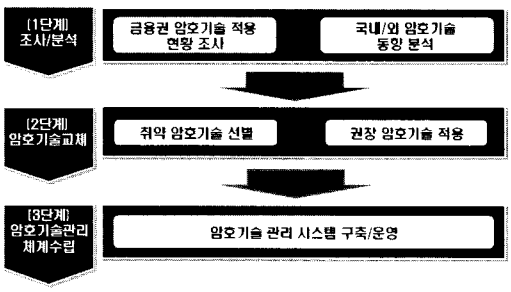
해쉬함수로 광범위하게 사용하고 있는 SHA-1의 경우, 해쉬함수 연산보다 적은 계산량에 의해 충돌이 탐색되어 그 안전성에 문제가 제기되고 있다〔4〕. 현실적인 측면에서 충돌 가능성이 쉽게 이루어지지는 않지만, 해쉬함수가 적용되는 상황에 따라 충돌에 의한 공격이 수행될 수 있으므로, 안전한 시스템 구축을 위해 충돌 가능성이 제기된 해쉬함수는 변경되어야 하는 것이 바람직하다.

IV. 금융권 암호기술의 안전성 강화에 관한 연구

전자금융거래에는 다양한 암호기술을 사용하고 있다. 예를 들어 전자금융거래 중 금융 자동화기기를 이용한 금융거래 시 PIN-PAD, 카드 리더기 등 입력장치로부터 기기내 관리프로그램까지 전송되는 금융정보, 기기와 호스트 서버간에 통신되는 금융정보에 대한 기밀성과 무결성을 제공하기 위해 암호기술이 활용되고 있다. 금융정보의 기밀성을 보장하기 위해 대칭키 암호를 사용하며, 무결성을 보장하기 위해서는 메시지인증코드나 공개키 암호를 이용한 전자서명이 이용되고, 암호키 교환을 위해서는 공개키 암호화 방식을 이용하여 암호키를 공유하고 있다. 대칭키 암호로 DES, 2-Key Triple DES, RC2, SEED, 전자서명 및 암호키 교환에서 사용되는 알고리즘으로는 128비트 RSA, 해쉬함수로는 SHA-1, MD5를 주로 사용하고 있다. 이와 같이 금융권에 적용된 다양한 암호기술은 전자금융거래 이용자의 주요 금융정보를 보호하는데 사용되고 있다. 하지만 현재 사용 중인 암호기술에 대해 암호연구가들은 MD5 해쉬 알고리즘의 취약성 발견으로 사용을 금할 것을 이미 경고하였으며, SHA-1 해쉬 알고리즘 사용 시 충돌쌍[4]을 발견할 가

3) 반도체의 집적밀도는 18~24개월마다 배로 증가

능성이 "전산적으로 불가능하지 않음"을 증명하였다. 이 외에도 암호학적인 분석으로 안전성 저하가 증명된 암호기술은 이미 국내·외 주요기관의 정보보호정책에 영향을 미쳐 사용 중인 암호기술을 변경하고 교체하는 과정을 추진하고 있다. 국내 금융권 보안 담당자 및 보안업계에서도 암호기술에 대한 안전성 결과를 주목하고 있고 이를 반영하고 있으나, 아직까지 금융권 암호기술을 관리하는 체계적인 시스템을 갖추지 못하고 있다. 이와 같이 금융 시스템에 적용된 암호기술이 알려진 공격에 취약한지 또는 국내외 주요기관에서 사용 제한을 권고하는 암호기술인지 등을 파악하여 권장된 암호기술로의 교체 작업이 금융권에서 고려되어야 할 것이다. 〔그림 1〕은 금융권에서 사용하고 있는 암호기술을 강화하기 위해 추진해야하는 방안을 각 단계별로 제시한 것이고, 이에 대한 자세한 설명은 다음과 같다.



〔그림 1〕 금융권 암호기술 강화를 위한 추진 방향

4.1 금융권 암호기술 적용현황 분석

암호기술의 안전성 저하 현상에 따라 금융권 암호기술 교체를 위해 국내·외 주요기관의 암호기술 안전성 평가결과에 대한 동향 및 금융권 암호기술 적용현황 파악이 수행되어야 한다. 최근까지 국내·외 주요기관에서는 암호기술의 안전성 평가결과에 대해 제시하였으며, 여러기관에서 발표한 평가결과를 수집하여 국내 금융권 현황에 적합한 형태로 재정립하는 과정이 필요하다. 우선 금융권 암호기술 적용현황 파악을 위해, 전자금융서비스를 모바일 뱅킹, 인터넷 뱅킹 등으로 분류하고, 각 전자금융서비스에 적용된 보안제품이 기밀성, 무결성, 부인봉쇄와 같은 보안서비스를 제공하기 위해 적용된 암호알고리즘, 암호키, 암호대상 등과 키관리를 위한 암호알고리즘, 공유방식, 갱신 주기 등 조사과정을 통해 금융권의 전반적인 암호기술을 조사하는 선행작업을 고려해야 한다. 이를 바탕으로 금융권에 적용된 암호알고리즘 중 '취약한 암호기술을 선별'해야 하며, 국내 금융권에 적용할 수 있도록 권장되는 금융권에 적용 가능한 암호기술에 대해 가이드라인을 제시하거나 표준화 작업을 고려해야 한다.

보안기능 중 기밀성 제공을 위해 적용되는 암호기술의 분류표 (예시)

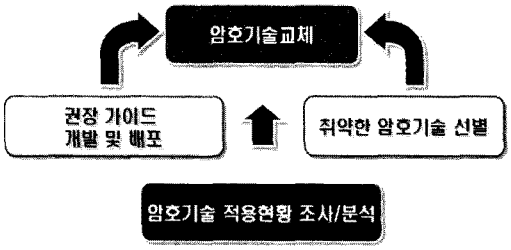
기밀성/무결성								
구간	매체	암호대상	암호대상 암호화용					
			비대칭키			대칭키		암호알고리즘 (운영모드)
			키길이 (bit)	키갱신 주기	공인인증서 사용여부	키길이 (bit)	키갱신 주기	
로컬 장비 구간								
네트워크 구간								
구간	매체	암호대상	키교환용					
			비대칭키			대칭키		암호알고리즘 (운영모드)
			키길이 (bit)	키갱신 주기	공인인증서 사용여부	키길이 (bit)	키갱신 주기	

보안기능 중 부인봉쇄 제공을 위해 적용되는 암호기술의 분류표 (예시)

부인봉쇄						
영역		전자서명 수행				
전자서명	이용자	서명/검증대상	공개키암호	해쉬암호	PKCS/OAEP	서명키길이
	금융기관					

이러한 과정 중 금융권에 적용 가능한 암호기술을 선정하는데 있어서 해당 애플리케이션에 적합한 최적의 암호키 길이 선정이 중요하며, 동일 수준의 안전성을 유지하는 암호알고리즘 중 애플리케이션의 구현성능에 맞춰 암호알고리즘을 선정하는 과정이 검토되어야 할 것이다. 이와 같은 선행작업〔그림 2〕을 통해 국내 금융기관 및 보안업체에서는 보안제품을 개발하고 적용하는데 있어 암호기술 사용에 대한 혼동을 사전에 방지할 수 있을 것이며, 암호기술 교체 시 상호연동성 등 수반될 수 있는 영향('암호기술 교체문제')을 최소화할 수 있을 것이다.

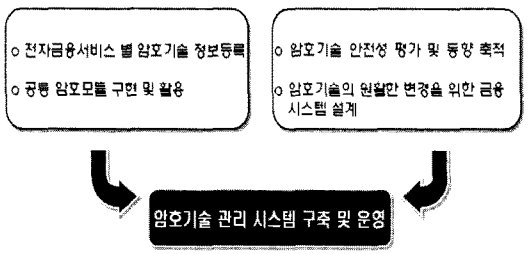
4) 해쉬함수는 다음 두 가지 사항을 만족할 때 안전한 것으로 간주함 (1) 특정 메시지 요약본에 해당하는 메시지를 찾거나, 또는 (2) 동일한 메시지 요약을 생성하는 2개의 서로 다른 메시지(충돌쌍)를 찾는 것은 전산적으로 불가능 함



〔그림 2〕 금융권 암호기술교체를 위한 선행작업

4.2 금융권 암호기술 관리

미국표준기술연구소에서는 2030년 이후 대칭키 암호로는 AES 암호 알고리즘 사용만을 권고하고 있지만 암호해독 기술 발전, 컴퓨터 성능 향상 등으로 인해 AES 암호알고리즘의 안전성 또한 DES와 같이 현저히 저하될 수 있다는 것이 암호 전문가들의 의견이다. 이처럼 현재 암호기술의 급격한 안전성 저하 현상 뿐만 아니라 향후 새로운 암호기술 개발 등으로 인해 해당 권고사항은 수시로 변경될 수 있을 것이다. 따라서 국내 금융시장에 적합한 암호기술의 권고, 그에 따른 변경시기 결정, 안전성이 저하된 암호알고리즘 발견 등을 수행하기 위해, 국내외 주요 기관에서는 검증된 암호기술의 안전성 평가 결과와 금융권 암호기술 관련 정보를 축적하여 금융권 암호기술을 지속적으로 연구하는 과정이 필요하다.



〔그림 3〕 금융권 암호기술 관리 시스템 구축 및 운영

이를 위해 신규 정보보호제품 및 구 제품의 정보 등록, 폐기 등 암호기술정보를 관리하는 '금융권 암호기술 관리 시스템' 구축에 대해 고려해야 한다. 금융권 암호기술 관리 시스템의 요소들은 금융권 암호기술 교체 작업을 위해 수행되는 금융권 암호기술 적용현황 파악으로부터 용이하게 구축될 수 있으며, 시스템을 구축한 후 등록된 보안제품에 대한 암호기술들의 수정사항에 대한 버전관리, 폐기된 보안제품에 대한 정보 삭제 등 시스템 운영에 대한 체계도 함께 고려되어야 할 것이다 〔그림 3〕. 금융권 암호기술 관리시스템 운영 중 안전성 평가가 현저히 저하된 암호기술이 발견된다면 취약한 암호기술을 사용 중인 금융기관에 정보제공을 통해 금융시스템의 안전성을 향상시킬 수 있을 것이며, 이를 위해 국내 산·학·연으로 이루어진 암호연구회를 구성하는 등 계속 발생하는 암호기술의 변화를 주시할 수 있는 환경 조성을 통해 금융기관 전체에 적용된 암호기술을 지속적으로 관리할 수 있는 체계를 갖추어 나가야 할 것이다.

V. 결 론

국제 주요기관 및 표준화 단체는 미국표준기술연구소의 안전성 평가 결과에 주목하고 있으며, 이에 따라 암호기술의 변경을 추진하고 있다. 암호기술의 안전성 저하 현상이 급격하게 발생하는 것은 아니지만 암호알고리즘의 사용기간 및 암호키 길이 등에 대한 권고사항이 분명하게 명시되어 있음에도 불구하고 금융권에서 이에 대응하지 않는다면 금융시스템의 신뢰도에 큰 영향을 미칠 것이다. 따라서 암호기술의 안전성 저하 현상에 따라 '금융권 암호기술 교체'가 발생될 수 있다는 것을 인식하고, 이에 대한 구체적인 방안을 선행적으로 연구해야 할 것이다.

참 고 문 헌

〔1〕 P. Oorschot and M.J. Wiener, "A known-plaintext attack on two-key triple encryption," EURO CRYPT'90, LNCS 473, pp. 318 - 325, 1990.

〔2〕 J. Kelsey, B. Schneier, and D. Wagner, "Related-key cryptanalysis of 3-WAY, Biham- DES, CAST, DES-X, NewDES, RC2, and TEA," ICICS, pp. 233 - 246, Nov. 1997.

〔3〕 S. Lucks, "Attacking Triple Encryption," Fast Software Encryption, LNCS 1372, pp. 239 - 253, 1998.

〔4〕 X. Wang and H. Yu, "How to Break MD5 and Other Hash Functions," EURO CRYPT'05, LNCS 3494, pp. 1-18, 2005.

〔5〕 한국은행 금융결제국, "금융분야의 안전한 암호이용에 대한 연구," p. 71, 2007년 11월.

[6] National Institute of Standards and Technology (NIST), "Cryptographic Algorithms and Key Sizes for Personal Identity Verification," Special Publication 800-78-1, p. 22, Aug. 2006.

[7] National Institute of Standards and Technology (NIST), "Recommendation for Key Management-Part 1: General (Revised)," Special Publication 800-57, p. 142, July 2007.