안전한 보안명령 전달을 위한 비행종단시스템용 암호화 장치 설계 요구사항

황수설*, 김명환*, 정혜승*, 오창열*, 마근수* 정회원

The cryptographic module design requirements of Flight Termination System for secure cryptogram delivery

Soosul Hwang*, Myunghwan Kim*, Haeseung Jung*, Changyul Oh* and Keunsu Ma*

요 약

본 논문에서는 우주발사체에 적용되는 비행종단시스템의 보안명령 입력을 위한 암호화 장치의 개념설계 결과와 개발 요구조건을 보였다. 암호화 장치는 명령신호를 생성하고 암호화하기 위한 명령생성장치와 암호화 명령신호를 연계장치에 입력하기 위한 명령입력장치로 구분하여 개발되도록 설계하였으며, 미국 NIST의 권고안과 한국인터넷진흥원(KISA)의 권고안을 참고하여 보안등급과 암호 알고리즘, 암호키 관리방안 등을 설정하였다. 암호화 장치는 AES-256 블록 암호화가 적용된 비밀키 알고리즘과 SHA-256의 해쉬 알고리즘을 적용하여 기밀성, 무결성, 가용성이 확보되도록 설계되었다. 설계된 암호화 장치는 우주발사체에 탑재되는 비행종단시스템의 보안명령 입력 용도로 활용되어 비행종단명령의 보안성과 비행종단시스템의 신뢰성 향상에 기여할 것으로 판단된다.

Key Words : Cryptographic Module, Security, Encryption, Decryption, Symmetric Key, Reliability

ABSTRACT

In this paper, we show the design requirements of the cryptographic module and its security algorithm designed to prevent the exposure of the command signal applied to Flight Termination System. The cryptographic module consists of two separate devices that are Command Insertion Device and Command Generation Device. The cryptographic module designed to meet the 3 principles(Confidentiality, Integrity and Availability) for the information security. AES-256 block encryption algorithm and SHA-256 Hash function were applied to the encrypted symmetric key encryption method. The proposed cryptographic module is expected to contribute to the security and reliability of the Flight Termination System for Space Launch Vehicle.

I. 서 론

정보 보호가 요구되는 시스템에 암호 알고리즘을 적용하기 위해서는 해당 시스템의 안전성 요구 수준을 확인하여 시스템이 요구하는 보안강도를 만족할 수 있는 암호 알고리즘이 선택되어야 한다. 또한, 암호화를 통한 정보의 보호가 필요한 시스템은 암호 알고리즘의 선택뿐만 아니라 비밀키의 크기 결정 및 정보의 기밀성을 보장할 수 있는 암호화된 정보와 비밀키의 유효기간 설정이 추가로 요구된다. 과거의 암호 방식에서는 사용되는 비밀키 뿐만 아니라 암호 알고리즘도 비밀로 하여 암호문의 비밀을 지키려고 하는 경우가 있었으나, 현대 암호 방식에서는 암호 알고리즘을 공개하도록 하고 있다. 이는 Auguste Kerckhoff가 1883년에 암호 시스템의 안전성에 대해 발표한 '비밀키를 제외한 암호 시스템의 모든 것이 공개되어도 암호화된 정보는 안전해야 한다'는 Kerckhoff의 원칙에 근거한다. 이렇게 함으로써 암호 방식의 안전성이 공개적으로 검토되도록 하여 암호 알고리즘의 안전성을 확보하고자 하는 것이다[1].

우주발사체에서 정보 보호가 특히 요구되는 분야는 비행종단시스템(FTS: Flight Termination System)이 대표적이다. 발사체에 탑재되는 비행종단시스템은 발사체에 발생될 수 있는 비정상 상태를 대비하기 위한 목적의 시스템으로,

*한국항공우주연구원 한국형발사체개발사업본부 발사체기술개발단 발사체전자팀
(sooseul@kari.re.kr, micele@kari.re.kr, hsjung@kari.re.kr, ocy@kari.re.kr, ksma@kari.re.kr), 교신저자 : 황수설
접수일자 : 2015년 8월 31일, 수정완료일자 : 2015년 9월 15일, 최종게재확정일자 : 2015년 9월 22일

발사체와 지상의 비행안전을 위해 필수적으로 탑재되어야 한다. 비행종단시스템은 적용 목적의 특수성에 의해 명령신호의 철저한 보안과 시스템의 안전성, 매우 높은 신뢰도가 요구된다[2]. 비행종단 동작은 명령전송을 위한 지상시스템과 명령을 수신하여 비행종단 기능을 수행하는 탑재시스템 간에 정해진 명령에 의해서만 동작하여야 하며, 이러한 명령이 외부에 노출되어 불순한 목적에 잘못 사용될 경우 심각한 사태를 초래할 수 있으므로 비행종단시스템과 관련된 명령의 형태, 명령신호의 조합, 적용 주파수 등 비행종단시스템과 관련된 모든 부분에 대해 각별한 보안이 요구된다.

보안정보의 관리에는 인적 관리방법과 물리적 관리방법이 적용될 수 있다. 인적 관리방법인 보안정보에 대한 정보 공유인원의 최소화 및 정보 공유자에 대한 보안서약서 작성을 통해 정보의 기밀성을 확보할 수 있고, 암호화 방식이 적용된 별도의 외부 전달수단을 통해 정보를 전달하는 물리적 관리방법을 적용하여 전달되는 정보의 무결성 및 가용성을 보장할 수 있다. 일반적인 경우, 인적 관리방법만으로도 일정 수준 이상의 보안은 유지될 수 있으나 정보의 전달과정에서 보안정보의 의도하지 않은 외부 유출 가능성은 여전히 존재하게 된다. 이러한 보안정보의 외부 유출 가능성을 차단하기 위해서는 보다 적극적인 관리방법이 요구된다. 인적 관리방법과 함께 물리적 관리방법이 함께 적용되면 정보에 대해 보다 강력한 보안이 가능해지고 보안정보의 외부 유출 가능성이 원천적으로 차단될 수 있다.

본 논문에서는 비행종단시스템에 적용되는 보안명령의 안전한 관리와 보안 유지를 위해 요구되는 암호화 장치의 설계시 고려사항을 보인다. 또한, 비행종단시스템의 보안명령 입력에 활용되기 위한 암호화 장치의 개념설계 결과 및 개발 요구조건을 보인다.

Ⅱ. 암호화 장치 설계시 고려사항

2.1 정보보안

정보보안이란 특정 정보 및 정보 시스템을 허가되지 않은 자에 의한 접근, 사용, 공개, 변경, 파괴 등으로부터 보호함으로써 정보의 기밀성, 무결성, 가용성을 제공하는 것을 말한다[3]. 즉, 정보보안은 정보나 시스템을 공격하고자 하는 자로부터 중요한 가치를 가지는 자산을 보호하는 것을 의미한다. 앞서 말한 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability)을 정보보안이 목표로 하는 3가지 핵심 원칙이라 말하며, 접근제어(Access Control), 인증(Authentication), 부인 방지(Non-repudiation) 등이 추가되어 정보보안의 안전성이 확보되어야 한다.

이러한 정보보안의 3가지 핵심 원칙은 서로 긴밀한 연관관계를 가지고 있다. 가용성 측면에서 보면 가용성을 높일수록 기밀성과 무결성은 유지되기 어려울 수 있고, 반대로 기밀성과 무결성을 높이다 보면 가용성이 유지되기 어렵다.

표 1. 정보보안을 위한 3가지 핵심 원칙

구분	내용	유사 개념	반대 개념
기밀성	인가된 사용자에게만 접근 허용	접근제어	노출, 공개
무결성	승인되지 않은 방법에 의한 정보 변경 보호	인증	변조, 위조
가용성	필요시 정보에 대한 접근 보장	부인방지	부인, 지체

그러므로 안전한 보안정책을 수립하기 위해서는 보안이 적용될 시스템의 안전성 수준과 시스템에 요구되는 보안강도를 정확히 파악하여 정보보안 원칙에 위배되지 않도록 하여야 한다. 정보보안을 위한 핵심 원칙을 만족시키기 위한 방법으로 암호 알고리즘 적용, 암호키 방식 및 암호키 크기 선정, 해쉬 알고리즘 적용, 장치 및 정보 공유자간 고유 식별번호 확인, 보안카드 인증 등 여러 가지 방법이 적용될 수 있다.

2.2 보안등급

정보보안을 위해서는 중요 보안정보를 보호하기 위해 해당 정보에 대한 중요도를 정확히 파악하고, 중요도에 따라 최선의 물리적/기술적/관리적 보안대책을 수립하여야 한다. 이를 위해 기밀정보 유출시 발생되는 피해 정도를 파악하여 정보에 대한 물리적/기술적 접근허용 범위를 판단하고, 정보의 중요도에 따른 보안등급을 설정하여 관리하여야 한다.

표 2. 기밀정보의 보안등급 설정[4]

등급	정의	접근허용 범위
Ⅰ	• 비공개 원칙의 정보 • 보안상 접근권한의 최소화가 요구되며 특정 관련자에게만 접근권한이 허용되는 정보 • 정보 유출시 대규모/치명적인 손실이 예상되는 정보	• 업무관련 특권 소수자에 한해 접근허용
Ⅱ	• 비공개 원칙의 정보 • 규정절차에 따른 허가된 업무관련자에 한해 접근이 허용되는 정보 • 정보 유출시 중규모/중대한 손실이 예상되는 정보	• 허가된 업무관련자에 한해 제한적 접근허용
Ⅲ	• 비공개 원칙의 정보 • 업무상 필요에 의해 업무관련자의 수시접근이 필요한 정보 • 정보 유출시 소규모/경미한 손실이 예상되는 정보	• 업무관련 정보 요청시 수시로 접근허용

모든 기밀정보는 비공개를 원칙으로 하며, 시스템이 요구하는 보안등급이 결정되면 시스템의 안전성 수준을 만족할 수 있는 보안강도가 설정되어야 한다. 여기서, 보안강도란 시스템에 적용된 암호 알고리즘이나 암호화/복호화를 위한 비밀키 또는 정보보안을 위해 적용된 여러 가지 방법의 취약성

을 찾아내는데 소요되는 작업량을 수치화한 것을 말한다[4]. 즉, 보안강도는 적용된 암호 알고리즘의 보안성을 해치기 위해 몇 번의 단위공격을 반복하여야 하는지를 정량적으로 표현한 것이다. 또한, 안전성 수준이란 시스템이 어느 정도의 보안강도를 만족하는지 판단하여 시스템에 적용된 안전성의 취약 여부를 판단하는 정성적 평가 방법을 의미한다.

2.3 암호 알고리즘

정보의 안전한 암호화를 위해서는 안전성이 검증되어 신뢰성이 보장된 암호 알고리즘을 선택하여야 한다. 암호 알고리즘은 크게 비밀키 알고리즘과 공개키 알고리즘으로 구분할 수 있다.

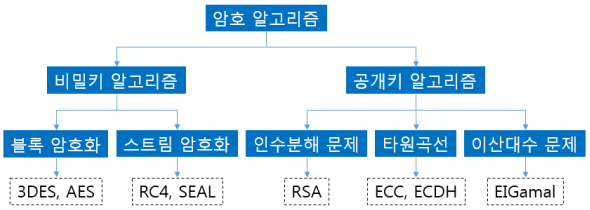


그림 1. 암호 알고리즘 분류

비밀키 알고리즘은 정보의 암호화와 복호화에 동일한 키가 적용되는 알고리즘으로 대칭키, 단일키 등과 같이 여러 가지 이름으로 불리어 진다. 비밀키 알고리즘을 통해 정보를 전달하기 위해서는 정보 공유자 간에 동일한 비밀키를 공유하고 있어야 한다. 외부에 노출되는 정보는 암호화된 정보이므로 비밀키를 모르는 상태에서는 노출된 내용만으로 정보를 확인할 수 없게 되므로 안전한 정보보안이 가능하게 된다. 비밀키 알고리즘에서는 암호화된 정보와 비밀키를 함께 전송해서는 안 된다. 따라서 암호문을 전달하는 경로와 비밀키를 전달하는 경로는 물리적으로 분리되어야 한다. 암호학에서는 이와 같이 서로 다른 경로를 통해 비밀키를 전달하는 것을 '비밀키 교환'이라고 하며, 적절한 비밀키 교환방법을 찾아 적용하는 것이 비밀키 알고리즘을 활용하는데 있어 가장 어렵고 중요한 문제이다. 비밀키 알고리즘은 정보 공유자가 많아지게 되면 비밀키의 개수 또한 늘어나게 되므로 다수의 정보 공유자가 필요한 시스템에서는 비효율적일 수 있다.

공개키 알고리즘은 비밀키 알고리즘과 달리 송신자와 수신자가 서로 다른 키를 사용하여 비밀 통신을 수행한다. 정보 공유자는 자신에게 전송하기 위해 사용될 키를 미리 공개하고, 공개된 키 정보로 암호화된 정보를 복호화할 수 있는 또 다른 비밀키를 보유하고 있음으로써 누구나 암호화할 수는 있으나 공개키에 대응되는 비밀키를 가진 당사자만이 정보를 올바르게 복호화할 수 있다는 특징을 가지고 있다. 송신자는 수신자의 공개키에 해당하는 정보를 사용하여 정보를 암호화하고 통신망을 통해 전송한다. 수신자는 자신의 공개키에 해당하는 비밀키로 암호화된 정보를 복호화하여 정보를 복원한다. 공개키 알고리즘은 정보 공유자간 키를 공유하지 않더라도 암호를 통한 안전한 통신을 한다는 장점을 가진다.

표 3. 암호 알고리즘 비교[5]

구분	비밀키 알고리즘	공개키 알고리즘
장점	• 암호화/복호화 속도 빠름. • 키 크기가 작음. • 알고리즘이 간단함.	• 키의 분배가 용이함. • 개인키만 관리하면 됨. • 여러 분야에 응용 가능함.
단점	• 사용자 수에 따라 관리 필요한 키의 개수도 변화됨. • 알고리즘에 따라 키 변화의 빈도가 높음.	• 암호화/복호화 속도 느림. • 키 크기가 큼. • 알고리즘이 복잡함.

암호 알고리즘은 암호화를 적용하는 방식에 따라 다양한 알고리즘이 적용될 수 있다. 비밀키 알고리즘은 암호화와 복호화를 수행하는 연산 방법에 따라 블록 암호화 방식과 스트림 암호화 방식으로 구분할 수 있으며 3DES 및 AES, RC4, SEAL 등의 알고리즘이 대표적으로 적용될 수 있다. 공개키 알고리즘은 수학적 난제를 기반으로 설계된 암호화 방식으로 큰 수의 인수분해의 어려움에 안전성을 둔 방식과 이산대수 문제의 어려움에 기반을 둔 방식 등이 대표적이며 RSA, ECC, ECDH, EIGamal 알고리즘 등이 적용될 수 있다. 암호 알고리즘을 선정하기 위해서는 데이터 보호를 위한 시스템의 보안강도가 먼저 결정되어야 하며 설정된 보안강도를 유지하기 위해 시스템이 갖추어야 하는 방식의 암호 알고리즘과 암호키의 선택이 이어져야 한다.

2.4 해쉬 알고리즘

해쉬 함수(Hash Function)는 임의의 길이를 갖는 문자열을 입력 받아 고정된 길이의 암호문(해쉬값)을 출력하는 일방향 함수를 말한다. 여기서, 일방향 함수란 결과값을 가지고 입력값을 구하는 것이 어려운 함수를 말하며 해쉬 함수가 이와 같은 일방향 함수에 해당한다[6]. 암호 알고리즘에는 키가 사용되지만, 해쉬 알고리즘에서는 키를 사용하지 않으므로 같은 입력에 대해서는 항상 같은 출력이 나오게 된다. 해쉬 알고리즘은 입력 문자열에 대해 항상 동일한 암호문을 출력하므로 입력된 문자열의 오류나 변조를 탐지할 수 있어서 승인되지 않은 방법에 의한 정보 변경을 보호하는 정보보안의 무결성을 제공하는 목적으로 적용이 가능하다.

해쉬값에 대한 서명이 원래 입력된 문자열에 대한 서명으로 인정되기 위해서는 같은 해쉬값을 갖는 또 다른 임의의 문자열을 찾아내기가 계산적으로 어려워야 한다. 해쉬 함수는 임의의 길이를 갖는 문자열을 입력받아 일정한 길이의 암호문(해쉬값)을 출력하므로 입력한 문자열은 서로 다르지만 같은 출력값을 가질 수도 있다. 이와 같이 서로 다른 입력값에 대해 동일한 출력값을 나타낸 경우에 해쉬 알고리즘에서 충돌(Hash Collision)이 발생하였다고 표현하며, 안전한 해쉬 알고리즘이 사용되기 위해서는 적용된 해쉬 함수의 충돌

을 찾아내는 것이 시간상으로나 비용상으로 불가능하도록 해쉬 알고리즘이 설계되어야 한다.

해쉬 알고리즘은 앞서 제시한 비밀키 알고리즘과 공개키 알고리즘에 비해 상대적으로 덜 알려져 있지만, 사용빈도 및 중요성에서는 두 알고리즘보다 높다고 할 수 있다. 해쉬 알고리즘은 임의의 길이를 갖는 난수 생성이나 메시지 인증 코드(MAC, Message Authentication Code)로도 사용될 수 있다.

2.5 암호키 관리

암호키 관리는 암호를 효과적으로 사용하기 위한 필수적인 요소이다. 기밀정보를 완벽한 방법을 통해 암호화하여 전달하여도 암호화/복호화에 적용된 암호키가 공격자에게 노출되면 높은 보안성을 갖는 암호 알고리즘이 적용되었다하더라도 기밀정보는 쉽게 유출되게 된다[4]. 기밀정보의 외부 유출을 차단하기 위해 암호문과 암호키는 물리적으로 분리된 경로를 통해 전달되어야 하며, 이를 위한 암호키의 분배 및 관리는 정보보안을 위해 중요하게 고려되어야 한다.

암호키 관리는 키의 전달 경로뿐만 아니라 암호 알고리즘에 적용된 암호키의 크기에 의해서도 영향을 받는다. 암호키는 크기가 길어짐에 따라 가능한 키의 경우의 수가 늘어나기 때문에 공격자가 올바른 암호키를 찾기 어렵게 된다. 암호키의 크기가 무한정 길어진다고 안전해지는 것은 아니다. 암호키의 크기가 길어진다는 것은 키를 알아내기 위한 공격자의 공격시도 시간이 지수적으로 늘어난다는 것을 의미할 뿐이며 충분한 시간이 제공된다면 어떠한 키 크기에 대해서도 적용된 암호키는 찾아낼 수 있다. 그러므로 안전한 암호키 관리를 위해서는 공격자가 가질 수 있는 계산 능력과 기밀정보의 보호기간, 지켜야 할 기밀정보의 가치 등을 고려하여 적절한 암호키 크기가 선택되어야 한다.

암호키의 기밀성에 대한 신뢰는 시간이 지남에 따라 감소하게 된다. 암호키의 유효기간은 정보 공유자가 암호키를 사용할 수 있는 기간 또는 특정 시스템에 주어진 암호키의 유효성이 유지되는 기간을 말하며, 암호키의 유효기간이 짧으면 그만큼 공격에 노출되는 시간이 짧으므로 정보보안이 향상된다. 암호키의 유효기간을 설정할 때는 키 노출을 야기하는 위험 요소와 키 노출에 따른 영향성 등을 함께 고려하여야 한다. 안전한 암호 알고리즘을 사용하였을 경우, 알고리즘이나 키 길이보다 암호키의 유효기간이 물리적, 절차적, 논리적 접근 보호에 대한 고려사항에 미치는 영향이 더 크므로 암호키 유효기간 설정에 신중을 기해야 한다[7].

미국의 국립표준기술연구소(NIST, National Institute of Standards and Technology)에서는 정보 보호를 위한 보안강도를 보안비트 크기에 따라 5가지(80, 112, 128, 192, 256 bit)로 나누고 있으며, 안전성 유지기간에 따른 유효한 암호키의 크기도 함께 제시하고 있다[4].

표 4. 알고리즘별 보안강도 및 안전성 유지기간 권고안

보안 비트	비밀키 알고리즘	공개키 알고리즘 (키 크기)		해쉬 알고리즘	안전성 유지기간
		RSA	ECC		
80	2DES	1024	160 ~ 223	MD5, SHA-1	~ 2010년
112	3DES	2048	224 ~ 255	SHA-224	~2030년
128	AES-128	3072	256 ~ 383	SHA-256	2030년 ~
192	AES-196	7680	384 ~ 511	SHA-384	
256	AES-256	15360	512 ~	SHA-512	

시스템의 요구조건에 따라 여러 가지 암호 알고리즘이 사용될 수 있다. 그리고 각 암호 알고리즘에서도 다양한 키 크기를 선택할 수 있다. 여기서 필요 이상으로 큰 키를 사용하게 되면 키의 생성 및 처리에 필요한 시간이 길어지게 되어 비효율적일 수 있다. 반면 작은 키를 사용하면 보안에 취약해질 수 있다. 그러므로 정보의 민감성 및 암호가 사용되는 환경 등에 따라 적합한 알고리즘과 키를 선택하여 사용하여야 한다. NIST에서 권고한 사항에 따르면 보안비트가 80비트인 알고리즘은 이미 안전성에 문제가 있다고 판단하고 있으므로 보안이 적용될 시스템의 향후 적용기간을 고려하여 적합한 보안비트에 해당하는 알고리즘을 선택하여야 한다[4].

Ⅲ. 비행종단시스템용 암호화 장치 설계

3.1 비행종단시스템 보안명령 입력 체계

현재 우주발사체의 비행종단시스템은 명령신호 결정권자가 명령신호의 조합과 명령코드를 선정하여 명령문서에 수기로 기록한 후 비행종단시스템 운용자에게 전달하는 명령신호 전달 체계를 가지고 있다. 전달된 명령문서는 비행종단시스템을 구성하는 장치의 제작 및 운용을 위해 보안정보를 공유하여야 하는 최소한의 정보 공유자에게 전달되어 탑재장치 및 지상장치에 명령코드가 최종적으로 입력되게 된다.

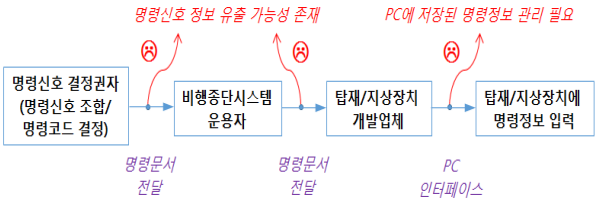


그림 2. 현재 적용되고 있는 비행종단명령 입력 체계

이와 같은 명령신호 전달 체계에서는 명령신호 결정권자에 의해 결정된 명령신호를 비행종단시스템 운용자와 탑재 및 지상장치 개발업체에게 전달하는 과정에서 명령정보의 외부 유출 가능성이 존재하며, 전달된 명령이 공용 컴퓨터를 통해 장치에 입력하게 된다면 컴퓨터에 저장된 명령정보가 외부에 유출될 가능성 또한 존재한다.

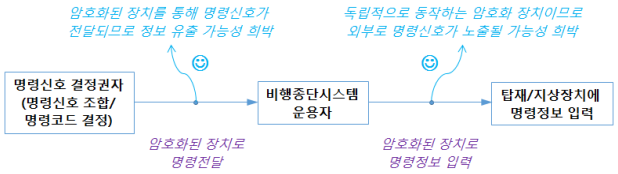


그림 3. 암호화 장치를 통한 비행종단명령 입력 체계

암호화 알고리즘이 적용된 외부 암호화 장치를 통한 비행종단명령 입력 체계에서는 명령신호 결정권자가 결정한 보안정보가 암호화된 장치에 저장되어 비행종단시스템 운용자에게 전달되므로 비행종단시스템 운용자조차도 결정된 명령정보를 알 수 없게 된다. 또한, 탑재 및 지상장치에 명령정보를 입력할 때에도 독립적으로 동작하는 외부 암호화 장치를 통해 입력되므로 명령정보가 외부에 노출될 가능성 또한 충분히 대비할 수 있다.

3.2 해외발사체에 적용된 보안명령 입력 체계

미국의 발사체에 적용된 비행종단시스템에서는 별도의 외부장치(ex. KYK-13, CYZ-10, KIK-13)를 이용하여 명령신호를 탑재장치와 지상장치에 입력하는 것으로 확인된다. 이러한 외부 입력장치 내에는 명령신호를 암호화 및 복호화할 수 있는 알고리즘을 장치 내부에 가지고 있어서 명령신호의 외부유출에 대해 원천적인 차단이 가능하며, 명령신호 결정권자는 비행종단시스템 운용자 누구와도 명령과 관련된 정보를 공유하지 않으므로 인적 보안 또한 가능하도록 운용되고 있다.

(a) KYK-13 (b) CYZ-10 (c) KIK-13

그림 4. 해외발사체에 적용된 암호화 장치 예

이와 같이 해외발사체에 적용된 암호화 장치에 대한 실체는 확인되고 있으나, 이 장치가 동작하기 위한 명령 형태나 동작 원리, 프래임 구조, 암호화 방식 등의 정보는 보안상의 이유로 한정적으로 공개되어 있다. 이와 같은 암호화된 명령입력장치는 우주발사체 분야 뿐만 아니라 군에서도 보안이 요구되는 통신시스템에 활용되어 정보 유출에 대비하고 있는 것으로 파악된다.

3.3 암호화 장치를 통한 보안명령 전달 체계 설계

비행종단시스템에 적용되는 명령정보는 명령 결정권자를 제외하고는 정보를 다루는 운용자조차 암호화된 정보의 원래 정보가 무엇인지 알 수 없어야 하는 기밀정보이다. 비행종단시스템은 이와 같은 적용 목적의 특수성에 의해 명령정보에 대한 높은 보안성이 요구되며, 명령의 생성부터 탑재 및 지상장치에 명령정보를 입력하기까지의 전 과정에 대해 철저한 보안관리가 요구된다.

비행종단시스템용 암호화 장치는 앞서 제시한 보안 요구사항을 만족시키기 위해 암호화 명령정보를 생성하는 명령생성장치와 연계장치에 명령정보를 전달하기 위한 명령입력장치로 각각 개발되어야 한다. 명령 결정권자는 명령생성장치를 통해 명령코드를 결정하고 명령신호를 조합하여 암호화 시킨 후 명령입력장치에 암호화된 명령신호를 전달한다. 명령입력장치는 암호화되어 전달받은 명령신호를 복호화하여 원래의 명령신호로 복원한 후 인증된 탑재 및 지상장치에 입력한다. 이와 같은 동작을 수행하기 위해 암호화 장치는 명령입력장치 기준으로 암호화된 명령신호를 입력받기 위한 수신모드와 탑재 및 지상장치에 복호화된 명령신호를 입력하기 위한 송신모드를 가지게 된다. 수신모드와 송신모드로 동작하기 위해서는 장치가 연결이 되었을 때 연계장치간 고유 식별번호 확인 등의 인증을 통해 허가된 장치인지의 확인 절차가 필요하다.

그림 5. 비행종단시스템용 암호화 장치 구성 및 운용 모드

수신모드에서 명령 결정권자는 명령생성장치를 이용하여 명령코드와 비밀키를 먼저 생성한다. 명령코드는 생성된 비밀키를 이용하여 암호화되어 명령입력장치에 입력된다. 명령정보는 명령입력장치에 암호화되어 입력된 상태로 비행종단시스템 운용자에게 전달되고, 생성된 비밀키는 별도의 저장 수단을 이용하여 또 다른 운용자에게 보안카드와 함께 전달된다. 탑재 및 지상장치에 생성된 명령정보를 입력하기 위한 송신모드에서는 고유 식별번호 확인을 통해 연계장치간 인증을 먼저 수행하고 보안카드 인증을 통해 명령입력장치에 접근한 운용자가 허가된 자인지 확인되어야 한다. 장치와 운용자의 인증이 확인되면 명령입력장치의 전달 경로와는 다른 경로를 통해 전달받은 비밀키를 이용하여 암호화된 명령정보를 복호화한 후 탑재 및 지상장치에 명령정보를 전달하게 된다.

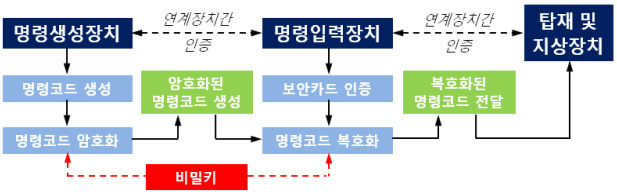


그림 6. 비행종단시스템용 암호화 장치 동작

이와 같이 암호화를 위한 명령생성장치는 표준화된 알고리즘을 이용하여 명령코드를 생성하고 안전성이 보장된 상태에서 인증된 장치에게로만 명령을 전송할 책임이 있으며, 명령입력장치는 명령을 전송받은 장치가 신뢰할 수 있는 장치이고 수신된 명령이 충분한 안전성과 신뢰성을 가진 정보인지 확인해야 하는 책임이 있다.

3.4 비행종단시스템용 암호화 장치 개념설계 결과

비행종단시스템용 암호화 장치는 정보보안의 3원칙을 만족하도록 설계되어야 한다. 이를 위해 암호화 장치는 기밀성 확보를 위해 암호 알고리즘을 적용하여 허가되지 않은 자에 의한 접근을 차단하도록 설계되었고, 해쉬 알고리즘을 적용하여 허가되지 않은 방식에 의한 정보 변조를 막아 무결성을 갖도록 하였다. 또한, 외부 명령입력장치 적용과 장치간 고유 식별번호의 교차확인을 통해 가용성이 확보되도록 설계하였다. 비행종단시스템에 적용되는 명령정보는 보안등급상 최상위 기밀정보에 해당하므로 접근권한의 최소화가 요구된다. 이를 위해 블록 암호화 방식을 응용한 비밀키 알고리즘을 적용하여 보안정보로의 접근이 업무와 관련한 소수인원에 한해 제한되도록 하였다. 암호화 장치를 통한 보안명령 생성은 최상위 명령 결정권자 1인에 의해 결정되므로 명령 생성자의 신분에 대한 인증은 요구되지 않고 명령의 전달과정에서 변조되지 않는다는 무결성 만이 주요한 고려사항이 된다. 이를 위해 해쉬 알고리즘을 적용하여 임의의 문자열 입력값을 난수 형태의 다양한 명령조합으로 한번에 만들어 내기 위한 용도와 메시지인증코드(MAC) 용도로 사용하였다. 암호키는 안전성 유지기간을 고려하여 충분한 보안강도를 가지는 112 비트 이상의 보안비트 알고리즘 중 선택되어야 한다. 이를 위해 256 비트의 보안비트를 가지는 AES-256 비밀키 알고리즘을 선택하였고, 보안비트는 낮으나 선택된 비밀키 알고리즘과 동일한 크기를 가져 응용상의 효율성이 확보될 수 있는 SHA-256 해쉬 알고리즘을 선택하였다.

표 5. 암호화 장치 개념설계 결과

구분	내용
보안등급	I 등급 (특권 소수자에 한해 접근 허용)
기밀성 확보	암호 알고리즘 통한 접근 제어
무결성 확보	해쉬 알고리즘 통한 위/변조 방지 및 인증
가용성 확보	외부 암호화 장치 적용을 통한 부인방지
암호화 장치 구성	명령생성장치, 명령입력장치
암호 알고리즘	비밀키 알고리즘
암호화 종류	블록 암호화 (AES-256)
해쉬 알고리즘	SHA-256
장치 인증	장치간 고유 식별번호 확인, 보안카드 인증
비밀키 관리	SD 메모리 장치 이용한 물리적 전달경로 분리
비밀키 유효기간	최대 5년

암호화 장치는 명령생성장치와 명령입력장치로 구분하여 개발되도록 설계하였다. 명령생성장치는 PC 기반의 명령생성 프로그램으로 구성되며 보안성 확보를 위해 검증된 알고리즘을 사용하여 암호화가 수행되어야 한다. 프로그램 운용은 허가된 사람에 의해서만 가능하여야 하며, 수행된 암호화 작업 내역은 암호화 작업 이후에 완전히 삭제되어야 한다. 명령입력장치는 명령생성장치로부터 입력받은 명령신호의 정상유무 판별 기능과 입력된 암호화 명령신호를 복호화 할 수 있는 알고리즘을 자체적으로 포함하고 있어야 한다. 또한 가용성 확보를 위해 연계장치간 고유 식별번호를 확인할 수 있어야 하며 고유번호의 불일치시 입/출력이 거부되는 기능을 가져야 한다.

표 6. 암호화 장치 개발 요구조건

구분	내용
명령생성장치	• PC 기반의 명령생성 프로그램 운용 • 보안성 확보를 위한 검증된 알고리즘 사용 • 명령신호 조합/명령코드 결정/암호화 기능 포함 • 명령입력장치의 고유번호 식별 기능 • 명령생성 프로그램은 허가된 사람에 한하여 접근 가능/허가된 PC에서만 실행 가능 • 암호화 작업내역은 작업 종료 후 완전 삭제
명령입력장치	• 명령생성장치로부터 입력받은 명령신호의 정상유무 판별 기능 • 입력된 암호의 복호화를 위한 자체 알고리즘 탑재 • 명령생성장치와 연계장치의 고유번호 식별 기능 • 고유번호 불일치시 입/출력 거부 기능 • 연계장치간 연결을 위한 물리적인 인터페이스 포함 • 독립적인 구동을 위한 배터리 탑재

Ⅳ. 결 론

본 논문에서는 우주발사체에 적용되는 비행종단시스템의 보안명령 입력을 위한 암호화 장치의 개념설계 결과와 개발 요구조건을 보였다. 비행종단시스템에 적용되는 명령정보는 최상위 기밀정보로 이러한 보안정보가 외부에 노출되어 잘못 사용되게 되면 발사체 및 지상안전에 심각한 피해를 가져올 수 있다. 이러한 기밀정보의 외부유출을 원천적으로 차단하기 위해서는 검증된 강력한 암호화 방식이 탑재되고 독립적인 구동이 가능한 암호화 장치가 개발되어 적용되어야 한다. 암호화 장치는 명령신호를 생성하고 암호화하기 위한 명령생성장치와 암호화 명령신호를 연계장치에 입력하기 위한 명령입력장치로 구분하여 개발되도록 설계하였으며, 미국 NIST의 권고안과 한국인터넷진흥원(KISA)의 권고안을 참고하여 보안등급과 암호 알고리즘, 암호키 관리방안 등을 설정하였다.

본 논문을 통해 설계된 암호화 장치는 요구 성능에 대한 상세설계를 통해 신뢰성과 보안성이 충분히 확인되면 가깝

게는 한국형발사체(KSLV-II)용 비행종단시스템의 비행종단명령 입력에 적용되어 해외 발사체에 적용된 수준의 보안성이 확보된 비행종단시스템 운영체계를 구축할 수 있으리라 판단된다.

참 고 문 헌

[1] 한국인터넷진흥원(KISA) 홈페이지, "암호이용활성화/ 암호소개," http://seed.kisa.or.kr/iwt/ko/index.do

[2] 황수설, 고정환, 이재득, "해외발사체 사례조사를 통한 FTS 명령방식 변천사 연구," 제11회 우주발사체기술 심포지움, pp. 283-289, 2010.

[3] USC Title 44, Chapter 35, §3542

[4] 한국인터넷진흥원(KISA), "암호이용 안내서," 2010.01

[5] 박영호, "공개키 암호,"물리학과 첨단기술, pp. 7-12, 2007.

[6] 한국인터넷진흥원(KISA), "암호이용활성화, 암호 키 관리 안내서," 2014.12

[7] 한국인터넷진흥원(KISA), "암호이용활성화, 암호기술 구현 안내서," 2013.12

저자

황 수 설(Soosul Hwang) **정회원**

- 1998년 2월 : 충남대학교 전파공학과 학사
- 2000년 2월 : 충남대학교 대학원 전파공학과 공학석사
- 2013년 2월 : 충남대학교 대학원 전파공학과 공학박사
- 2000년 1월 ~ 2002년 2월 : 삼성전자 무선사업부 연구원
- 2002년 3월 ~ 현재 : 한국항공우주연구원 한국형발사체개발사업본부 발사체기술개발단 발사체전자팀 선임연구원

<관심분야> : 비행종단시스템(FTS), 무선통신 및 시스템, RF 능동회로 설계, 능동 제어회로 설계

김 명 환(Myunghwan Kim) **정회원**

- 2003년 2월 : 충남대학교 전기공학과 학사
- 2005년 2월 : 충남대학교 대학원 전기공학과 공학석사
- 2005년 3월 ~ 현재 : 한국항공우주연구원 한국형발사체개발사업본부 발사체기술개발단 발사체전자팀 선임연구원

<관심분야> : 발사체 전력시스템, 탑재장치 점검시스템

정 혜 승(Haeseung Jung) **정회원**

- 2000년 2월 : 부산대학교 컴퓨터공학과 학사
- 2002년 2월 : 부산대학교 컴퓨터공학과 석사
- 2002년 3월 ~ 현재 : 한국항공우주연구원 한국형발사체개발사업본부 발사체기술개발단 발사체전자팀 선임연구원

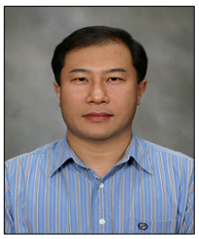
<관심분야> : 모델기반 임베디드 시스템 개발, 텔레메트리 시스템

오 창 열(Changyul Oh) **정회원**

- 1990년 2월 : 충남대학교 전자공학과 학사
- 1992년 2월 : 충남대학교 대학원 전자공학과 공학석사
- 2011년 2월 : 충남대학교 대학원 전자공학과 공학박사
- 1992년 3월 ~ 2000년 6월: 국방과학연구소 선임연구원
- 2000년 6월 ~ 2001년 6월: 한국전자통신연구원 선임연구원
- 2001년 7월 ~ 현재 : 한국항공우주연구원 한국형발사체개발사업본부 발사체기술개발단 발사체전자팀 책임연구원

<관심분야> : 무선통신 및 시스템, 추적안테나, 전파전파

마 근 수(Keunsu Ma) **정회원**



- 1990년 2월 : 충남대학교 전기공학과 학사
- 1994년 2월 : 충남대학교 대학원 전기공학과 공학석사
- 2003년 2월 : 충남대학교 대학원 전기공학과 공학박사
- 1994년 3월 ~ 현재 : 한국항공우주연구원 한국형발사체개발사업본부 발사체기술개발단 발사체전자팀 책임연구원/팀장

<관심분야> : 위성체 및 발사체 전자시스템, 공진형 DC/DC 컨버터