AnyLink-S 접속고객을 위한 암호화모듈 사용 안내

**# 암호화 적용 범위**

대우증권에서 제공하는 AnyLink-S(Open Interface System)은 KISA(한국정보통신진흥회)의 Seed암호화를 이용한다.

- Data(주문,조회) 전송 시 **계좌(고객)비밀번호**

를 대우증권에서 고객별로 배포한 UserKey를 이용하여 아래와 같이 Data Header(100Byte)의 Password 컬럼에 저장하여 전송하여야 한다.

|  |  |  |  |
| --- | --- | --- | --- |
| Item | | Length | Description |
| 1 | Data ID | Char (8) |  |
| 2 | Data Length | Char (6) |  |
| 3 | Return Code | Char (6) |  |
| 4 | Password | Char (30) |  |
| 5 | Filler | Char (50) |  |

**1. LINK(로그인) 메시지 전송 시**

# 대우증권에서 배포한 **세션ID**를 평문으로 Password필드에 전송한다.

|  |  |  |  |
| --- | --- | --- | --- |
| Communication Header (60 byte) | Data Header (100 byte) | | |
|  | **Password (30Byte)** |  |

**2. DATA 메시지 전송 시**

# 주문(조회) 시 해당 **고객계좌의 비밀번호**를 암호화하여 Password필드에 전송한다.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Communication Header (60 byte) | Data Header (100 byte) | | | Data Body (n byte) |
|  | **Password** |  |

Ps.) 조회 시에 Data Body에 비밀번호 필드가 존재하는 경우에, Data Body는 동일한 Password를 입력하거나, space(옵션)로 채워서 전송한다.

**# SEED암호화 모듈 다운로드 절차 안내**

- SEED 홈페이지 (http://seed.kisa.or.kr/)



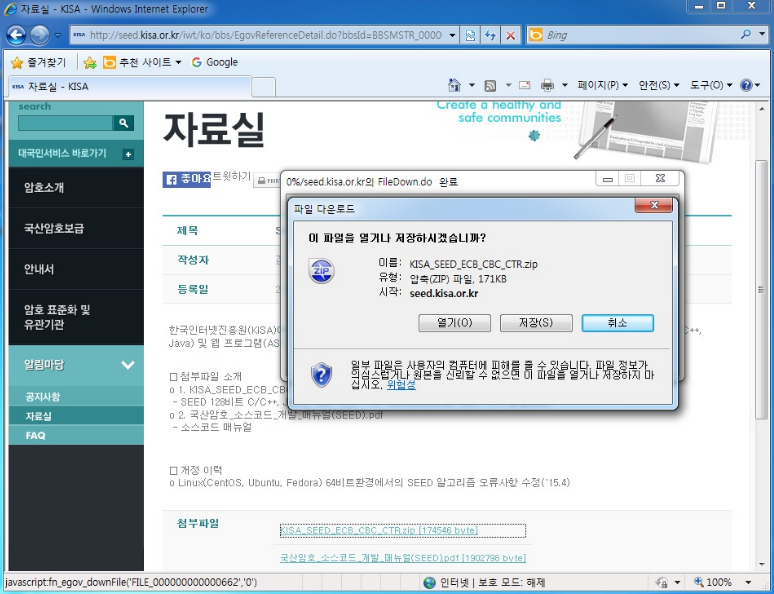
- SEED안내 페이지-> 알림마당 -> 자료실로 이동한다.



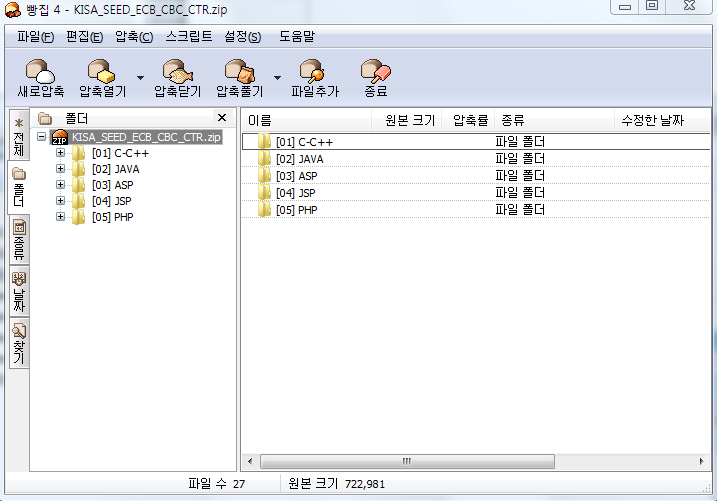
- “SEED 블록암호 알고리즘 소스코드(C/C++,JAVA,ASP,JSP,PHP)” 버튼을 클릭한다.



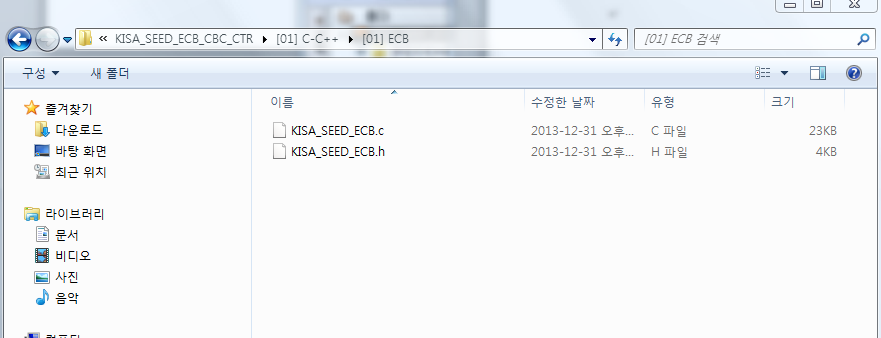
- “KISA\_SEED\_ECB\_CBC\_CTR.zip”을 다운로드한다.



- “KISA\_SEED\_ECB\_CBC\_CTR.zip”파일의 암축을 푼다.



- SEED 운영모드는 ECB방식을 취한다. KISA\_SEED\_ECB.h 및 KISA\_SEED\_ECB.c



**# SEED암호화 모듈 사용법**

가. 첨부 파일 (SEED샘플프로그램.zip)

- BASE64.c : BASE64 알고리즘 구현파일

- BASE64.h : BASE64 알고리즘 Header파일

- KISA\_SEED\_ECB.c : SEED 암호화 알고리즘 구현 파일

- KISA\_SEED\_ECB.h : SEED 암호화 알고리즘 헤더 파일

- Makefile : 샘플 프로그램 Makefile (RedHat Linux 6.x)

- seedtest.c : 샘플 프로그램

나. 암호화 함수

**void SeedEncText(BYTE \*lpKey, BYTE \*lpPwd, BYTE lpEncPwd[]);**

- lpKey : null termination으로 정의된 문자열 암호화용 비밀키(최대 16자)

- lpPwd : 암호화를 위한 평문. Null termination으로 정의된 16자 미만의 비밀번호.

최대 15자이다.

'- lpEncPwd : 암호화된 계정계 패스워드. 24자리의 BASE64로 변환된 문자열 데이터가

전달된다. 최소한 45 Byte이상의 버퍼

다. 복호화 함수

**void SeedDecText(BYTE \*lpKey, BYTE \*lpBase64, BYTE lpPwd[]);**

- lpKey : null termination으로 정의된 문자열 암호화용 비밀키(최대 16자).

SeedEncText()에서 사용한 값과 같은 값이어야 한다.

- lpBase64 : SeedEncText()에서 암호화된 문자열. 24자리로 고정된 길이의 데이터이다.

- lpPwd : 복호화된 계정계 비밀번호. SeedEncText()에서 전달된 lpPwd와 동일한 값이

전달된다. 최소한 33 Byte의 버퍼가 할당되어야 한다.

라. 샘플 프로그램 사용방법

- 암호화 시

seed –e encKey accPwd

- 복호화 시

seed –d encKey accPwd

-사용 예

# **make**

gcc -g -c seedtest.c

gcc -g -c KISA\_SEED\_ECB.c

gcc -g -c BASE64.c

gcc -g -pthread -Wall -o seed seedtest.o KISA\_SEED\_ECB.o BASE64.o

# **seed -e oiskey 0101001**

OrgData: '0101001'

EncText: 'Gxw69amqWScTpX7kTChAsw=='

# **seed -d oiskey Gxw69amqWScTpX7kTChA**

OrgData: 'Gxw69amqWScTpX7kTChAsw=='

DecText: '0101001

STEP 1) **SEED\_KeySched** 함수로 대우증권에서 배포한 UserKey를 이용해 RoundKey를 생성한다.

STEP 2) **SEED\_Encrypt** 함수로 대우증권에서 배포한 세션ID를 RoundKey를 이용해 암호화 한다.

1. LINK 시 전송 시