(19)대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。Int. Cl.[7]
H04L 9/00

(11) 공개번호 10-2005-0086088
(43) 공개일자 2005년08월30일

(21) 출원번호 10-2004-0012422
(22) 출원일자 2004년02월24일

(71) 출원인 이주원
서울 중구 신당동 844 남산타운 아파트 4동 1801호

(72) 발명자 이주원
서울 중구 신당동 844 남산타운 아파트 4동 1801호

(74) 대리인 이수웅
박경완

심사청구 : 있음

(54) 문자 메시지 암호화 방법 및 장치

요약

본 발명은 이동 통신 단말기에 관한 것으로서, 더욱 자세하게는 이동 통신 단말기에서 문자 메시지를 암호화하고 복호화할 수 있는 방법 및 장치에 관한 것이다. 이동 통신 단말기에 적용되는 문자 메시지 암호화 방법에 있어서, 본 발명에 따른 문자 메시지 암호화 방법은 a) 발신자에 의하여 원천 텍스트가 입력되면 코드 테이블에 정해진 위치값에 따라 각각의 원천 텍스트에 대한 원천 위치값이 정의되는 단계, b) 암복호화 키값에 따라 원천 위치값이 암호화 위치값으로 변환되는 단계, c) 코드 테이블에 따라 암호화 위치값에 해당하는 암호화 텍스트가 정의되는 단계, d) 암복호화 키값과 암호화 텍스트가 전송되는 단계, e) 코드 테이블을 이용하여 암호화 텍스트 각각의 암호화 위치값이 검색되는 단계, f) 암복호화 키값을 이용하여 검색된 암호화 위치값 원천 위치값으로 변환되는 단계 및 g) 코드 테이블을 이용하여 상기 암호화 위치값으로부터 변환된 원천 위치값에 따라 원천 텍스트가 정의되는 단계를 포함하는 것을 특징으로 한다.

이와 같은 본 발명은 코드 테이블과 암복호화 키값을 이용하여 간단하게 문자 메시지를 암호화하고 복호화함으로써 문자 메시지에 대한 정보 누출 및 사생활 침해를 막을 수 있을 뿐만 아니라 이동 통신 단말기에 설치가 용이하고 비용 증가의 문제를 해결할 수 있다.

대표도

도 1

명세서

도면의 간단한 설명

도 1은 본 발명에 따른 문자 메시지 암호화 방법의 순서도이다.

도 2는 본 발명에 따른 문자 메시지 암호화 방법을 위한 코드 테이블이다.

도 3은 본 발명에 따른 문자 메시지 암호화 장치의 블록구성도이다.

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 이동 통신 단말기에 관한 것으로서, 더욱 자세하게는 이동 통신 단말기에서 문자 메시지를 암호화하고 복호화할 수 있는 방법 및 장치에 관한 것이다.

일반적인 이동 통신 단말기는 음성 통화뿐만이 아니라 문자 메시지 송수신, 멀티미디어 데이터 송수신과 같은 다양한 기능을 수행할 수 있다. 이와 같은 이동 통신 단말기의 여러 기능 중 음성 통화는 고도의 비화기술을 이용하여 발신자의 정보가 외부로 유출되는 것을 막는다. 그러나 일반적인 이동 통신 단말기가 문자 메시지를 수신할 경우, 문자 메시지는 이동 통신 단말기의 메모리에 그대로 남아 있기 때문에 타인에게 쉽게 노출되는 문제점이 있다.

또한 발신자가 틀린 번호로 전화를 걸었을 경우, 발신자는 상대방을 확인할 수 있기 때문에 불필요한 정보의 유출을 막을 수 있다. 이에 반해 발신자가 틀린 번호로 문자 메시지를 보낼 경우, 발신자는 문자 메시지가 정확히 원하는 사람에게 전송되었는지 확인하기가 어려울 뿐만 아니라 원하지 않는 사람에게 문자 메시지가 전송되고 원하지 않는 사람이 문자 메시지를 완벽하게 볼 수 있기 때문에 정보 유출 및 사생활 침해의 위험성이 상존하고 있다.

이와 같은 문제를 해결하기 위하여 컴퓨터용 암호화 프로그램을 이동 통신 단말기에 설치할 경우, 컴퓨터용 암호화 프로그램은 이동 통신 단말기에 탑재되기에는 컴퓨터용 암호와 프로그램의 사이즈가 너무 클 뿐만 아니라 프로그램의 가격 또한 비싸기 때문에 경제성이 떨어진다는 문제점이 발생한다.

발명이 이루고자 하는 기술적 과제

본 발명은 상기와 같은 문제점들을 해결하기 위한 것으로, 이동 통신 단말기에 설치가능한 문자 메시지 암호화 방법 및 암호화 장치를 제공하기 위한 것이다.

발명의 구성 및 작용

상기 목적을 달성하기 위하여 이동 통신 단말기에 적용되는 문자 메시지 암호화 방법에 있어서, 본 발명에 따른 문자 메시지 암호화 방법은 a) 발신자에 의하여 원천 텍스트가 입력되면 코드 테이블에 정해진 위치값에 따라 각각의 원천 텍스트에 대한 원천 위치값이 정의되는 단계, b) 암복호화 키값에 따라 원천 위치값이 암호화 위치값으로 변환되는 단계, c) 코드 테이블에 따라 암호화 위치값에 해당하는 암호화 텍스트가 정의되는 단계, d) 암복호화 키값과 암호화 텍스트가 전송되는 단계, e) 코드 테이블을 이용하여 암호화 텍스트 각각의 암호화 위치값이 검색되는 단계, f) 암복호화 키값을 이용하여 검색된 암호화 위치값 원천 위치값으로 변환되는 단계 및 g) 코드 테이블을 이용하여 상기 암호화 위치값으로부터 변환된 원천 위치값에 따라 원천 텍스트가 정의되는 단계를 포함하는 것을 특징으로 한다.

또한, 이동 통신 단말기에 적용되는 문자 메시지 암호화 장치에 있어서, 본 발명에 따른 문자 메시지 암호화 장치는 a) 송신되는 문자 메시지를 구성하는 원천 텍스트에 해당하는 전기 신호를 생성하는 키 입력부, b) 텍스트가 위치값에 따라 정의된 코드 테이블을 저장하는 메모리부, c) 코드 테이블을 통하여 전기 신호에 해당하는 원천 텍스트와 원천 텍스트에 해당하는 원천 위치값을 생성하고 암복호화 키값을 이용하여 원천 위치값에 대한 암호화 위치값과 암호화 위치값에 따른 암호화 텍스트를 생성하는 암호화 기능과, 수신받은 암복호화 키값과 코드 테이블을 이용하여 수신된 암호화 텍스트를 원천 텍스트로 변환하는 복호화 기능을 수행하는 제어부, d) 제어부로부터 입력된 암호화 텍스트와 암복호화 키값을 송신 처리하는 TX 처리부, e) 암호화 텍스트와 암복호화 키값을 수신 처리하는 RX 처리부, f) TX 처리부에 의하여 송신 처리된 신호를 송신하기에 적합한 RF 신호로 대역 변환한 후 안테나로 인가하고, RF 신호로 대역 변환된 신호를 수신하여 RX 처리부로 전달하는 RF 송수신부 및 g) 발신자에 의하여 작성된 문자 메시지, 수신된 암호화 텍스트 및 복호화된 원천 텍스트를 표시하는 표시부를 포함하는 것을 특징으로 한다.

이하, 본 발명의 실시예를 첨부된 도면을 참조하여 상세히 설명하고자 한다.

도 1은 본 발명에 따른 문자 메시지 암호화 방법의 순서도이고, 도 2는 본 발명에 따른 문자 메시지 암호화 방법을 위한 코드 테이블이다.

먼저 발신자에 의하여 원천 텍스트가 입력되면 코드 테이블에 의하여 원천 위치값이 정의된다(S110). 예를 들어, 발신자가 'AQ'라는 문자 메시지를 작성하여 전송한다고 가정한다. 도 1에 도시된 코드 태이블에서 원천 텍스트 A에 해당하는 원천 행번호 04와 원천 열번호 02가 정의된다. 또한, 상기 코드 태이블에서 원천 텍스트 Q에 해당하는 원천 행번호 05와 원천 열번호 02가 정의된다.

원천 위치값이 정의되면 암복호화 키값에 따라 원천 위치값이 암호화 위치값으로 변환된다(S120). 즉, 원천 행번호와 원천 열번호와 같은 원천 위치값이 정의되면, 암복호화 키값에 따라 암호화 행번호와 암호화 열 번호가 정의된다.

다시 말해서, 암복호화 키값이 0001이면, 원천 행번호 04는 그대로 유지되고 원천 열 번호 02는 암호화 열번호 03이 된다. 또한, 원천 행번호 05는 그대로 유지되고 원천 열 번호 02는 암호화 열번호 03이 된다.

이 때, 암복호화 키값은 미리 저장된 다수 개의 암복호화 키값 중에서 하나가 임의로 선택된다.

따라서, 암호화 위치값의 생성으로 원천 텍스트는 암호화 텍스트로 변환된다(S130). 즉, 원천 텍스트 A는 암호화 텍스트 B로 암호화된다. 따라서, 원천 텍스트 A는 암호화 텍스트 B로 암호화되고, 원천 텍스트 Q는 암호화 텍스트 R로 암호화된다.

이와 같이 발신자에 의하여 작성된 AQ라는 문자는 본 발명에 따른 암호화 방법에 따라 BR로 암호화되어 암복호화 키값 00001과 더불어 수신자에게 전송된다(S140). 따라서, 수신자는 AQ라는 문자를 보는 것이 아니라 암호화된 BR이라는 문자를 처음 보게 된다.

이후 수신자의 이동 통신 단말기는 암호화된 문자 메시지와 같이 전송된 암복호화 키값 0001을 이용하여 암호화된 문자 메시지를 복호화한다. 즉, 수신자의 이동 통신 단말기는 암복호화 키값 0001이 발신자의 이동 통신 단말기에서 수행한 동작의 역동작을 함으로써 암호화된 문자 메시지를 복호화한다.

다시 말해서, 암복호화 키값 0001은 발신자의 이동 통신 단말기에서는 원천 위치값인 원천 열번호를 1증가시키는 것을 의미하지만 수신자의 이동 통신 단말기에서는 암호화 위치값인 암호화 열변호를 1감소시키는 것을 의미한다.

S140에서 암호화 텍스트 및 암복호화 키값을 수신한 수신자의 이동 통신 단말기는 암호화 텍스트에 해당하는 암호화 위치값을 생성한다(S150). 즉, 수신자의 이동 통신 단말기가 암호화된 문자 메시지 BR을 수신하면, B에 해당하는 암호화 행번호 04 및 암호화 열번호 03와 R에 해당하는 암호화 행번호 05 및 암호화 열번호 03이 도 1의 코드 테이블에 따라 생성된다.

이와 같이 암호화 위치값이 생성되면 수신자의 이동 통신 단말기는 수신된 암복호화 키값에 따라 암호화 위치값을 원천 위치값으로 변환한다(S160). 즉, 암호화 행번호 04 및 암호화 열번호 03은 암복호화 키값 0001에 따라 원천 행번호 04와 원천 열 번호 02로 복호화된다. 또한, 암호화 행번호 05 및 암호화 열번호 03은 암복호화 키값 0001에 따라 원천 행번호 05와 원천 열번호 02로 복호화된다.

이후 코드 테이블에 따라 원천 위치값에 해당되는 원천 텍스트가 생성됨으로써 복호화 과정이 끝난다(S170). 즉, 도 1의 코드 테이블에 따라 원천 행번호 04와 원천 열 번호 02에 해당하는 A로 정의되고 원천 행번호 05와 원천 열번호 02에 해당하는 Q로 정의되어 복호화 과정이 끝난다.

본 발명의 실시예에서는 암복호화 키값이 미리 저장된 다수 개의 암복호화 키값 중에서 임의로 선택되는 것이 기재되어 있으나 한 개의 암복호화 키값이 미리 설정되어 있을 수도 있다. 또한, 발신자가 문자 메시지를 전송할 때마다 암복호화 키값을 직접 입력하여 문자 메시지와 함께 전송할 수도 있다.

또한, 본 발명의 실시예에서는 암복호화 키값이 원천 행번호는 그대로 유지하여 암호화 행번호가 형성되고 원천 열번호는 그 다음의 열번호로 암호화 열 번호가 생성되는 것을 의미하고 있으나, 원천 행번호의 증가나 대각 방향으로의 행번호 및 열 번호의 증가 등과 같이 다양한 의미가 가능한 것은 물론이다.

이와 같은 본 발명에 따른 문자 메시지 암호화 방법은 코드 테이블 및 암복호화 키값만으로 암호화가 진행되기 때문에 프로그램의 사이즈가 작아 이동 통신 단말기에 적합하다.

도 3은 본 발명에 따른 문자 메시지 암호화 장치의 블록구성도이다. 도 3에 도시된 바와 같이 본 발명에 따른 문자 메시지 암호화 장치는 키 입력부(310), 메모리부(320), 제어부(330), TX 처리부(340), RX 처리부(350), RF 송수신부(360) 및 표시부(370)를 포함한다.

〈키 입력부〉

키 입력부(310)는 송신되는 문자 메시지를 구성하는 원천 텍스트에 해당하는 전기 신호를 생성한다.

〈메모리부〉

메모리부(320)는 텍스트가 위치값에 따라 정의된 코드 테이블을 저장한다. 이 때, 메모리부(320)는 텍스트의 위치값을 변환하는 복수 개의 암복호화 키값을 저장할 수도 있다.

〈제어부〉

제어부(330)는 메모리부(320)에 저장된 코드 테이블을 통하여 전기 신호에 해당하는 원천 텍스트와 원천 텍스트에 해당하는 원천 위치값을 생성하고 암복호화 키값을 이용하여 원천 위치값에 대한 암호화 위치값과 암호화 위치값에 따른 암호화 텍스트를 생성하는 암호화 기능과, 수신받은 암복호화 키값과 코드 테이블을 이용하여 수신된 암호화 텍스트를 원천 텍스트로 변환하는 복호화 기능을 수행한다.

이 때, 제어부(330)는 메모리부(320)에 저장된 복수 개의 암복호화 키값 중 임의로 하나의 암복호화 키값을 선택하여 암호화 기능과 복호화 기능을 수행할 수 있다.

또한, 제어부(330)는 미리 메모리부(320)에 저장된 특정 암복호화 키값을 이용하여 암호화 기능과 복호화 기능을 수행할 수 있다.

마지막으로 제어부(330)는 문자 메시지 작성시 발신자에 의하여 조작된 키 입력부(310)로부터 전송된 암복호화 키값을 입력받아 암호화 기능과 복호화 기능을 수행할 수 있다.

〈TX 처리부〉

TX 처리부(340)는 제어부(330)로부터 입력된 암호화 텍스트와 암복호화 키값을 송신 처리한다. 여기서 송신 처리란 기저 대역 신호에 대해 변조, 주파수 상승 변환 등을 행하는 동작을 말한다.

〈RX 처리부〉

RX 처리부(350)는 수신 처리된 신호를 입력하여 주파수 하강 변환 및 복조 등의 수신 처리를 행한다.

〈RF 송수신부〉

RF 송수신부(360)는 TX 처리부(340)에 의하여 송신 처리된 신호를 송신하기에 적합한 RF 신호로 대역 변환한 후 안테나로 인가하고, RF 신호로 대역 변환된 신호를 수신하여 RX 처리부(340)로 전달한다.

〈표시부〉

표시부(370)는 발신자에 의하여 작성된 문자 메시지, 수신된 암호화 텍스트 및 복호화된 원천 텍스트를 표시한다.

이와 같은 본 발명에 따른 문자 메시지 암호화 장치는 코드 테이블과 암복호화 키값을 이용하여 간단하게 문자 메시지를 암호화 할 수 있기 때문에 이동 통신 단말기에 적합할 뿐만 아니라 비용 문제를 해결할 수 있다.

이와 같이, 본 발명이 속하는 기술분야의 당업자는 본 발명이 그 기술적 사상이나 필수적 특징을 변경하지 않고서 다른 구체적인 형태로 실시될 수 있다는 것을 이해할 수 있을 것이다. 그러므로 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며 한정적인 것이 아닌 것으로서 이해해야만 한다.

본 발명의 범위는 상기 상세한 설명보다는 후술하는 특허청구범위에 의하여 나타내어지며, 특허청구범위의 의미 및 범위 그리고 그 등가개념으로부터 도출되는 모든 변경 또는 변형된 형태가 본 발명의 범위에 포함되는 것으로 해석되어야 한다.

발명의 효과

이상에서와 같이 본 발명은 코드 테이블과 암복호화 키값을 이용하여 간단하게 문자 메시지를 암호화하고 복호화함으로써 문자 메시지에 대한 정보 누출 및 사생활 침해를 막을 수 있을 뿐만 아니라 이동 통신 단말기에 설치가 용이하고 비용 증가의 문제를 해결할 수 있다.

(57) 청구의 범위

청구항 1.

이동 통신 단말기에 적용되는 문자 메시지 암호화 방법에 있어서,

발신자에 의하여 원천 텍스트가 입력되면 코드 테이블에 정해진 위치값에 따라 상기 각각의 원천 텍스트에 대한 원천 위치값이 정의되는 단계;

암복호화 키값에 따라 원천 위치값이 암호화 위치값으로 변환되는 단계;

상기 코드 테이블에 따라 상기 암호화 위치값에 해당하는 암호화 텍스트가 정의되는 단계;

상기 암복호화 키값과 상기 암호화 텍스트가 전송되는 단계;

상기 코드 테이블을 이용하여 상기 암호화 텍스트 각각의 암호화 위치값이 검색되는 단계;

상기 암복호화 키값을 이용하여 상기 검색된 암호화 위치값 원천 위치값으로 변환되는 단계;

코드 테이블을 이용하여 상기 암호화 위치값으로부터 변환된 원천 위치값에 따라 원천 텍스트가 정의되는 단계를 포함하는 것을 특징으로 하는 문자 메시지 암호화 방법.

청구항 2.

제1항에 있어서,

상기 암복호화 키값은 암호화 과정에서는 상기 원천 위치값의 위치 이동을 의미하고, 복호화 과정에서는 암호화 위치값에서 원천 위치값으로의 이동을 의미하는 것을 특징으로 하는 문자 메시지 암호화 방법.

청구항 3.

제1항에 있어서,

상기 암복호화 키값은 미리 저장된 다수 개의 암복호화 키값 중에서 하나가 임의로 선택되어 암호화 과정이 수행되고 전송되는 것을 특징으로 하는 문자 메시지 암호화 방법.

청구항 4.

제1항에 있어서,

상기 암복호화 키값은 한 개의 암복호화 키값이 미리 설정되어 암호화 과정이 수행되고 전송되는 것을 특징으로 하는 문자 메시지 암호화 방법.

청구항 5.

제1항에 있어서,

상기 암복호화 키값은 발신자가 문자 메시지를 전송할 때마다 암복호화 키값을 직접 입력하여 암호화 과정이 수행되고 전송되는 것을 특징으로 하는 문자 메시지 암호화 방법.

청구항 6.

이동 통신 단말기에 적용되는 문자 메시지 암호화 장치에 있어서,

송신되는 문자 메시지를 구성하는 원천 텍스트에 해당하는 전기 신호를 생성하는 키 입력부;

텍스트가 위치값에 따라 정의된 코드 테이블을 저장하는 메모리부;

상기 코드 테이블을 통하여 상기 전기 신호에 해당하는 원천 텍스트와 상기 원천 텍스트에 해당하는 원천 위치값을 생성하고 암복호화 키값을 이용하여 원천 위치값에 대한 암호화 위치값과 암호화 위치값에 따른 암호화 텍스트를 생성하는 암호화 기능과, 수신받은 암복호화 키값과 코드 테이블을 이용하여 수신된 암호화 텍스트를 원천 텍스트로 변환하는 복호화 기능을 수행하는 제어부;

상기 제어부로부터 입력된 암호화 텍스트와 암복호화 키값을 송신 처리하는 TX 처리부;

상기 암호화 텍스트와 상기 암복호화 키값을 수신 처리하는 RX 처리부;

상기 TX 처리부에 의하여 송신 처리된 신호를 송신하기에 적합한 RF 신호로 대역 변환한 후 안테나로 인가하고, RF 신호로 대역 변환된 신호를 수신하여 상기RX 처리부로 전달하는 RF 송수신부;

발신자에 의하여 작성된 문자 메시지, 수신된 암호화 텍스트 및 복호화된 원천 텍스트를 표시하는 표시부를 포함하는 것을 특징으로 하는 문자 메시지 암호화 장치.

청구항 7.

제6항에 있어서,

상기 암호화 키값은 상기 메모리부에 복수 개 저장되고 상기 제어부는 상기 메모리부에 저장된 복수 개의 암복호화 키값 중 하나를 선택하여 암호화 과정을 수행한 후 상기 선택된 암복호화 키값을 송신하는 것을 특징으로 하는 문자 메시지 암호화 장치.

청구항 8.

제6항에 있어서,

상기 암호화 키값은 상기 메모리부에 한 개 저장되고 상기 제어부는 상기 메모리부에 저장된 한 개의 암복호화 킷값을 이용하여 암호화 과정을 수행한 후 상기 암복호화 키값을 송신하는 것을 특징으로 하는 문자 메시지 암호화 장치.

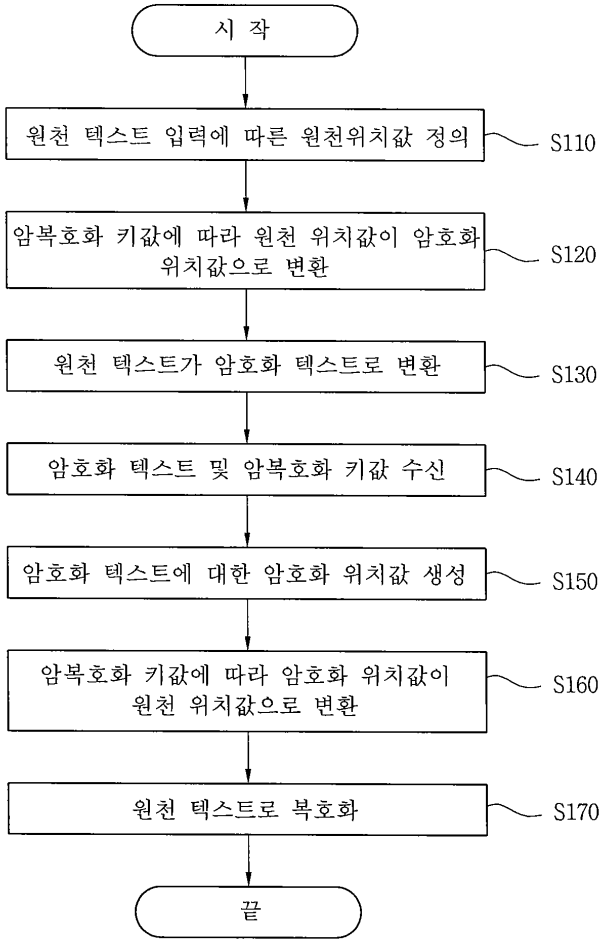
청구항 9.

제6항에 있어서,

상기 제어부는 문자 메시지 작성시 발신자에 의하여 조작된 상기 키 입력부로부터 전송된 암복호화 키값을 입력받아 암호화 기능과 복호화 기능을 수행하는 것을 특징으로 하는 문자 메시지 암호화 장치.

도면

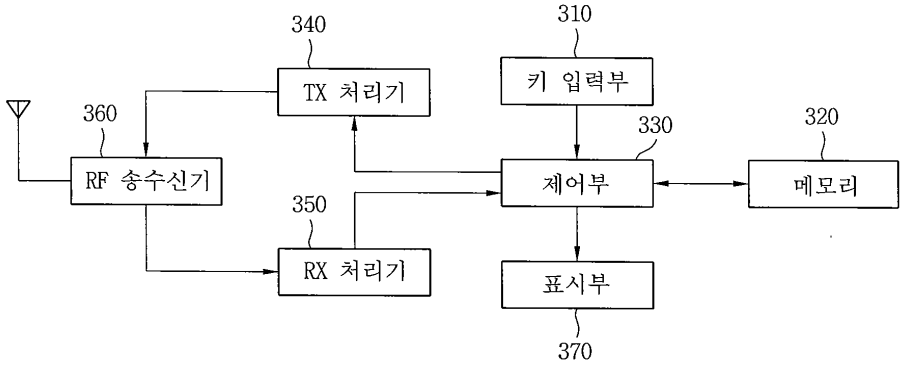
도면1



도면2

열번호 \ 행번호	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
01																
02					A	Q										
03					B	R										
04					C	S										
05					D	T										
06					E	U										

도면3


340
310
TX 처리기
키 입력부
360
330
320
RF 송수신기
제어부
메모리
350
RX 처리기
표시부
370