2025 암호분석경진대회

4번 문제

A5-GMR-1은 ETSI 표준인 GMR-1 위성 통신 표준에 사용되는 스트림 암호로 2012년 B.Driessen 연구팀이 단말기를 역공학하여 알고리즘을 밝혀냈다. A5-GMR-1은 master key K 와 frame number N 을 입력받아 keystream z 를 생성한다.[1]

$$z = enc(K, N)$$

다음과 같은 방식으로 생성된 암호문 집합이 ciphertext.bin으로 주어졌을 때, 마스터 키와 평문을 복원하시오.[2]

① 평문 p를 160-bit 단위로 나눈다.

$$p \rightarrow p_0 \mid p_1 \mid p_2 \mid \cdots$$

② 160-bit 단위로 인코딩을 적용한다. 인코딩 전체 과정을 나타내는 generating matrix를 G라 하면,[3]

$$p_0 \mid p_1 \mid p_2 \mid \cdots \rightarrow G^t \cdot p_0 \mid G^t \cdot p_1 \mid G^t \cdot p_2 \mid \cdots$$

③ scrambling bits s를 각각 XOR 한다.[4]

$$G^t \cdot p_0 \mid G^t \cdot p_1 \mid G^t \cdot p_2 \mid \cdots \rightarrow G^t \cdot p_0 \oplus s \mid G^t \cdot p_1 \oplus s \mid G^t \cdot p_2 \oplus s \mid \cdots$$

④ A5-GMR-1으로 생성한 keystream을 XOR한다. 이때, master key K는 동일하고, frame number는 연속된 수로 간주한다.

$$G^t \cdot p_0 \oplus s \mid G^t \cdot p_1 \oplus s \mid G^t \cdot p_2 \oplus s \mid \cdots \rightarrow G^t \cdot p_0 \oplus s \oplus enc(K, N_0) \mid G^t \cdot p_1 \oplus s \oplus enc(K, N_0 + 1) \mid G^t \cdot p_2 \oplus s \oplus enc(K, N_0 + 2) \mid \cdots$$

[추가 조건]

- $N_0 = 9867$
- 암호문은 2개의 error-bit를 포함하고 있음

[참고 사항]

[1] A5-GMR-1 알고리즘은 논문 Driessen, Benedikt, et al. "Don't trust satellite phones: A security analysis of two satphone standards." 2012 IEEE Symposium on Security and Privacy. IEEE, 2012. 또는 code_open.cpp를 참고하시오.

[2] code_open.cpp 는 일부가 가려진 ciphertext.bin 생성 코드이다.

[3, 4] 메시지 암호화 과정은 GMR-1 표준과 다를 수 있으니 generating matrix G 와 scrambling bit s 는 반드시 code_open.cpp에 제공된 값을 사용하시오.