2019 국가암호공모전 (Ⅱ-A) 분야

문제

공군에서 전자서명이 붙은 메시지들을 입수하였는데, 통신자들이 전자서명의 은닉채널을 이용하여 중요한 정보를 전달하고 있다는 첩보가 있다. 사용된 전자서명은 DSA(Digital Signature Algorithm)이며, 다음과 같은 파라미터들을 사용하고 있다.

p =
4349445962213346771005425232845727838336252528805558665990590240470749947810140632785570086210529055607857683115467490199117548707954653733811730248891247
q = 501741228604902886824541911451531811838214568727771965446042258609702237208 17
g =
2174582142019644155276818137638393001160821529179916986818524855155980721678000683379339584218075071275840823045973601487223201645328337396122493007683309

DSA에 사용되는 해시 함수는 SHA256이다.

다음은 입수한 메시지와 전자서명 쌍들이다.

Dear G, I am beginning to feel guilty for not having replied to your letters sooner : the sad truth is that I have nothing serious to say about them...
19138a8168a15ec87668 67e3250e61f92ce02ad33b2b6f6f9e21d63b34889165, 2811ba689e7c0c72798e0c23ea5c0676a75e7cf841c7e088835657e863374b2f

My dear S, Lately I have been thinking again about the general formalism of (Weil)cohomology and homology of schemes, and so doing, it seems to me that I have managed to find the correct definition of homotopic invariants.
102c9ed2ff0fe669a36639b71869f8a3a20868f6a29a898995aef5ac43116cea, 2811ba689e7c0c72798e0c23ea5c0676a75e7cf841c7e088835657e863374b2f

Dear G, How are the categories? I read in the Tribu that you are in the processof writing them. Is this true, and have you temporarily abandoned the Multiplodocus? I would also like to know how the latter is getting on, and if we can count on a rapid publication.
29630c9018e65a541aa4a865c66106ec746328669841d05cb0519e8c50bfe04d, 2811ba689e7c0c72798e0c23ea5c0676a75e7cf841c7e088835657e863374b2f

My dear S, Choquet has probably received the corrections of the proofs for Gauthier-Villars by now. I asked that 100 reprints of my article be sent to you, since there is no point sending them here to Harvard.
19138a8168a15ec8766867e3250e61f92ce02ad33b2b6f6f9e21d63b34889165, 1a5d2b618387de2e8bdc5b1a684d0153a45b0c51e2fa8a99b5d0510b58de1461

Dear G, Your letter makes me want to take stock of what I am doing with localfields J.-P. Serre : The results stated in this letter were published in [Se60b]and [Se61a]
2a7a22486cb5b0562832ca2ea4a59deb50ff8a041ca22742b20c40cab6e78688, 2811ba689e7c0c72798e0c23ea5c0676a75e7cf841c7e088835657e863374b2f

문제 : 위의 메시지와 서명들을 분석하여 숨겨진 정보를 찾아내라. 풀이과정을 암호학적으로 정당화하라. 숨겨진 정보는 어떠한 사건과 관련이 있는가?

참고사항 :

1. 주어진 각각의 메시지의 범위는 알파벳과 특수기호를 포함한 문장의 첫 문자부터 마지막 문자까지이다. 예를 들어 첫번째 메시지는 Dear G, I am beginning to feel guilty for not having replied to your letters sooner : the sad truth is that I have nothing serious to say about them...와 같이 네모로 둘러싸인 부분을 의미하며 그 SHA256 해시값은 다음과 같다 :
3e33f8ef50fb32f6d62734c17f074798365dbfd51c7f301e7ae11bb9d0c2af3e

2. 사용된 DSA 알고리즘에 관해서는 'FIPS PUB 186-4' 문서를 참조하라.