

Prova G2 – 2020.1 – PARTE II – Prazo 48h – (15h de 24/6/2020 a 15h de 26/6/202)
Total: 3,0 Pontos

A Delta Info Task Force recrutou você para participar de uma missão secreta com o objetivo de quebrar um dos criptogramas necessários para desativar uma bomba relógio cuja localização é desconhecida. O setor de telemática conseguiu interceptar o canal de comunicação utilizado para comandar o sistema de controle de ativação e desativação do artefato. No entanto, para enviar a sequência de desativação para o artefato, é necessário conhecer os 13 códigos secretos dos 13 criptogramas apresentados no painel de controle. Sabe-se que este modelo de artefato utiliza uma chave criptográfica comum a todos os criptogramas.

Em sua última missão, o agente Brasília conseguiu obter informações sigilosas sobre o algoritmo criptográfico e a chave criptográfica, conforme mostrado na mensagem transcrita abaixo:

Brasília: Delta-Info na escuta? Delta-Info na escuta? Aqui é o agente Brasília...câmbio...
Delta-Info: Na escuta, Brasília, prossiga...câmbio...
Brasília: Conseguimos informações cruciais para a desativação do artefato...câmbio...
Delta-Info: Excelente, Brasília, prossiga...câmbio...
Brasília: 00: DELTA ECHO SIERRA
01: CHARLIE BETA CHARLIE
02: PAPA KILO CHARLIE SIERRA CINCO
03: KILO ECHO YANKEE SIERRA ECHO ECHO DELTA
04: SIERRA KILO YANKEE WHISKEY ALFA LIMA KILO ECHO ROMA UNO NOVE SETE SETE
05: INDIA VICTOR
06:(estática)
Delta-Info: Mensagem copiada parcialmente, Brasília...prossiga 06...câmbio...
Delta-Info: Mensagem copiada parcialmente, Brasília...prossiga 06...câmbio...
Brasília: Brasília desligando...over...

Desde então, nenhum outro contato foi estabelecido com o agente Brasília. Na avaliação do setor de investigação e análises da Delta-Info, (i) todas os criptogramas têm uma probabilidade de 99,9% de serem gerados a partir de textos planos contendo o texto "Star Wars"; (ii) os 13 códigos secretos correspondem respectivamente aos valores IV (Initialization Vector) de cada um dos 13 criptogramas; e (iii) os 13 códigos secretos são formados apenas por caracteres numéricos (vetor de caracteres ASCII). Esse setor da Delta-Info tem grau de confiabilidade superior a 95% em todas as suas análises

Sua missão é determinar um dos 13 códigos secretos com a técnica de força bruta no prazo de 48h. Você deve desenvolver um programa em linguagem Java que deve receber a *semente da chave criptográfica*, o *texto plano do parcial conhecido* e o *criptograma em hexadecimal* na linha de argumento. O programa desenvolvido deve ser enviado por e-mail para delta-info@inf.puc-rio.br.

A designação do seu codinome nesta missão está na tabela abaixo. Seu criptograma está no site da Delta Info Task Force, no endereço: <http://www.inf.puc-rio.br/~anderson/Delta-Info> Use este site para entrar o código secreto que você descobrir e aguarde pela sua validação. Para acessar o site use a sua matrícula e o seu codinome **sem acentuação**.

| Agente | Codinome |
|--------------------|------------|
| BRUNO MARINHO | Acre |
| FERNANDO BERNARDO | Amazonas |
| GABRIEL CARVALHO | Pará |
| GUSTAVO CONTREIRAS | Tocantins |
| IAGO FARROCO | Piauí |
| INGRID ORNELLAS | Ceará |
| JESSICA CESARIO | Pernambuco |
| JOAO PEDRO | Alagoas |
| JOAO VICTOR | Sergipe |
| MATHEUS LOURENCO | Bahia |
| PHILIPPE JOSE | Rio |
| PILAR BAPTISTA | Parana |
| THIAGO NICACIO | Goiás |

Boa Investigação!