



Prova G2 – 2023.1 – PARTE II – (Não Presencial)
Prazo 48h – (15h de 26/6/2023 a 15h de 28/6/2023)
Total: 2,0 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 24 códigos secretos dos 24 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? 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: ALFA 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 DOIS ZERO UNO NOVE
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...câmbio final...

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: Episode"; (ii) os códigos secretos correspondem respectivamente aos valores IV (Initialization Vector) de cada um dos criptogramas; e (iii) os códigos secretos são formados apenas por caracteres numéricos de 0 a 9 (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 24 códigos secretos com a técnica de força bruta no prazo de 48h. Você deve desenvolver um programa em linguagem Java que deve receber (i) a *semente da chave criptográfica*; (ii) o *texto plano parcial* conhecido; e (iii) o *criptograma em hexadecimal* na linha de argumento. O programa desenvolvido deve ser enviado por e-mail para delta@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: <https://delta.inf.puc-rio.br> Use este site para entrar o código secreto que você descobrir e aguarde pela sua validação. Para acessar o site use a sua matrícula como ID e o seu codinome **sem acentuação**.

Agente	Codinome	Agente	Codinome
ANDRE COSTA DE ANDRADE	Alemanha	LEONARDO MONTEIRO MASTRA FONTOURA	Australia
DANIEL MENEZES C L DOS PASSOS	Canada	LUCCA BUFFARA DE ALMEIDA	Finlandia
DANIEL SCHREIBER GUIMARAES	Belgica	LUIZ FELIPE DA SILVEIRA C AUGUSTO	Grecia
GABRIEL BANAGGIA DE SOUZA	Dinamarca	MARIA CAROLINA ESTEVES DE AZEVEDO	Argentina
GABRIEL VIANNA SOLDANI	Egito	MATHEUS PEREIRA KULICK	Italia
GUILHERME DE MORAES VASSALLO	Irlanda	SOLENN BOULARD	Franca
IAN GERALDI CORDEIRO	Croacia	THEO FALCATO RIBEIRO P DE ATHAYDE	Espanha
ISABELLA LOPES CARMO DOS SANTOS	Escocia	THEO NECYK AGNER CALDAS	Bulgaria
JOÃO PEDRO GUIMARÃES SOARES	Hungria	THIAGO GIOSO FERNANDES	Austria
JOSÉ ALBERTO ROMANO	Brasil	THIAGO LEVIS ALAMBERT RODRIGUES	China
JULIO NECYK CAVALCANTI MAIA	Japao	THOMAS ADDIS JUNQUEIRA BOTELHO	Holanda
LAURA MENDONCA DA GLORIA LUZ	Chile	WALLACE SILVA DE FREITAS	India

Boa Investigação!