

**Extrair componentes de uma chave encriptada de um parceiro na LMK variant.**

Índice

[1. Problema 3](#_Toc35626406)

[2. Solução 3](#_Toc35626407)

[2.1. LMK Variant criar uma chave ZMK. 3](#_Toc35626408)

[2.2. No Crypto fazer oTriple-Des[reverso](EBC) 4](#_Toc35626409)

[2.3 No BP-Tools - Cryptographic Calculator 4](#_Toc35626410)

[2.3. Na sua LMK Variant criar uma chave MC-AC . 4](#_Toc35626411)

[3. Release Notes 5](#_Toc35626412)

# Problema

Extrair componentes de uma chave encriptada de uma LMK variant de um parceiro.

# Solução

## LMK Variant criar uma chave ZMK.

|  |
| --- |
| Online-AUTH>GC  Enter LMK id [0-1]: 0  Enter key length [1,2,3]: 2  Enter key type: 000  Enter key scheme: u  Clear component: 92C8 AD1C F2A7 312F 5E8A 7554 B964 8F8A  Encrypted component: UFE96 7EBB 5121 9CF0 9BEF A168 BB65 77DA  Key check value: 01E256  Online-AUTH>gc  Enter LMK id [0-1]: 0  Enter key length [1,2,3]: 2  Enter key type: 000  Enter key scheme: u  Clear component: E33B B6A2 08EA A732 2CDA 46AD 76B3 B6C2  Encrypted component: U992F 7D55 C12A 30E9 EC75 B0DD 3C3C 91AD  Key check value: AB898F  Online-AUTH>fk  Enter LMK id [0-1]: 0  Enter key length [1,2,3]: 2  Enter key type: 000  Enter key scheme: u  Enter component type [X,H,T,E,S]: x  Enter number of components [1-9]: 2  Enter component 1: 92C8 AD1C F2A7 312F 5E8A 7554 B964 8F8A  Component 1 check value: 01E256  Continue? [Y/N]: y  Enter component 2: E33B B6A2 08EA A732 2CDA 46AD 76B3 B6C2  Component 2 check value: AB898F  Continue? [Y/N]: y  Encrypted key: U88F8 7A3F E0C3 816F ED34 A698 41A4 3229  Key check value: E2B603  EXTRAIR ATRAVÉS DE UM XOR NO CRYPTO CHAVE EM CLARO  CLEAR KEY 71F31BBEFA4D961D725033F9CFD73948 |

## No Crypto fazer oTriple-Des[reverso](EBC)

|  |
| --- |
| Através do Crypto  Imput: UEAA1BB92D5FF1A24002859C2F25AA7EF (chave mk-ac(109) do parceiro)  Key 16 bits (clear key) 71F31BBEFA4D961D725033F9CFD73948  Output  **F6DE3F1C2DB14D8A77D7CBACCF21CD1A** |

## No BP-Tools - Cryptographic Calculator

|  |
| --- |
| Através do **Keyshare Generator**  Combined Key  **F6DE3F1C2DB14D8A77D7CBACCF21CD1A**  **Two part key**  **Componente 01 2309B05279192DD5B23825AA9E400482**  **Componente 02 D5D78F4E54A8605FC5EFEE065161C998** |

## Na sua LMK Variant criar uma chave MC-AC .

|  |
| --- |
| Usar os componentes localizados no passo anterior  Online-AUTH>fk    Enter LMK id [0-1]: 0  Enter key length [1,2,3]: 2  Enter key type: 109  Enter key scheme: u  Enter component type [X,H,T,E,S]: x  Enter number of components [1-9]: 2    Enter component 1: \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  Component 1 check value: C3A1F2  Continue? [Y/N]: y    Enter component 2: \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  Component 2 check value: FAB00E  Continue? [Y/N]: y      Encrypted key: U7839 FE30 E7C3 27FD 754D 03F4 C3FC F872  Key check value: 9CE489 |

# Release Notes

|  |  |  |
| --- | --- | --- |
| **Autor** | **Descrição** | **Data** |
| Bruno Araujo |  | 20/03/2020 |
|  |  |  |