Rezolvare WORLD WAR II

Flag-ul problemei este: FIICODE25{BERLINHASFALLENRETREATALLREMAININGTROOPSTODEFENDTHEPARTSOFTHECOUNTRYTHATWESTILLHOLDDONOTSURRENDER}  
  
 Pentru a-l obține, trebuie să decriptăm mai întâi fișierul audio care ne-a fost dat. Ne dăm seama din audio că mesajul a fost criptat folosind Morse Code. Așa că introducem wav-ul pe site-uri care îl putem decripta și obținem: THE BATTLE OF THE BULGE, ALSO KNOWN AS THE ARDENNES COUNTEROFFENSIVE, WAS THE LAST MAJOR GERMAN OFFENSIVE CAMPAIGN ON THE WESTERN FRONT DURING WORLD WAR II, AND TOOK PLACE FROM 16 DECEMBER 1944 TO 25 JANUARY 1945. IT WAS LAUNCHED THROUGH THE DENSELY FORESTED ARDENNES REGION OF WALLONIA IN EASTERN BELGIUM, NORTHEAST FRANCE, AND LUXEMBOURG, TOWARDS THE END OF THE WAR IN EUROPE. THE OFFENSIVE WAS INTENDED TO STOP ALLIED USE OF THE BELGIAN PORT OF ANTWERP AND TO SPLIT THE ALLIED LINES, ALLOWING THE GERMANS TO ENCIRCLE AND DESTROY FOUR ALLIED ARMIES AND FORCE THE WESTERN ALLIES TO NEGOTIATE A PEACE TREATY IN THE AXIS POWERS'

FAVOR.

XDADDDAAADAXDGGDGAADGDDFXDFGAGFAFGGGAGDFDXFFAXDXGDXDGDDXAXFAFDGGAAGFAFGFDGAFXFFGXDGGGAAAFAFAADAGDGDDXXAADDGAGDFFXDAGFDXFFGGGGGGGDGFDDGADXGDXXDXXAAXAGGDFGDDAAAGAGDXADDGXDGXGDDXADXDAAFAGGXGGDGGDAGGGXGFGDDGGXXGX BEFORE THE OFFENSIVE THE ALLIES WERE VIRTUALLY BLIND TO GERMAN TROOP MOVEMENT. DURING THE LIBERATION OF FRANCE, THE EXTENSIVE NETWORK OF THE FRENCH RESISTANCE HAD PROVIDED VALUABLE INTELLIGENCE ABOUT GERMAN DISPOSITIONS. ONCE THEY REACHED THE GERMAN BORDER, THIS SOURCE DRIED UP. IN FRANCE, ORDERS HAD BEEN RELAYED WITHIN THE GERMAN ARMY USING RADIO MESSAGES ENCIPHERED BY THE ENIGMA MACHINE, AND THESE COULD BE PICKED UP AND DECRYPTED BY ALLIED CODE-BREAKERS HEADQUARTERED AT BLETCHLEY PARK, TO GIVE THE INTELLIGENCE KNOWN AS ULTRA. IN GERMANY SUCH ORDERS WERE TYPICALLY TRANSMITTED USING TELEPHONE AND TELEPRINTER, AND A SPECIAL RADIO SILENCE ORDER WAS IMPOSED ON ALL MATTERS CONCERNING THE UPCOMING OFFENSIVE. 42 THE MAJOR CRACKDOWN IN THE WEHRMACHT AFTER THE 20 JULY PLOT TO ASSASSINATE HITLER RESULTED IN MUCH TIGHTER SECURITY

RVDAYFTNLGXCPBQWHIOKUMZES AND FEWER LEAKS. THE ATTACKS BY THE SIXTH PANZER ARMY'S INFANTRY UNITS IN THE NORTH FARED BADLY BECAUSE OF UNEXPECTEDLY FIERCE RESISTANCE BY THE U.S. 2ND AND 99TH INFANTRY DIVISIONS. KAMPFGRUPPE PEIPER, AT THE HEAD OF SEPP DIETRICH'S SIXTH PANZER ARMY, HAD BEEN DESIGNATED TO TAKE THE LOSHEIM-LOSHEIMERGRABEN ROAD, A KEY2: SECONDWORLDWAR ROUTE THROUGH THE LOSHEIM GAP, BUT IT WAS CLOSED BY TWO COLLAPSED OVERPASSES THAT GERMAN ENGINEERS FAILED TO REPAIR DURING THE  
 Odată decriptat, observăm că avem 3 string-uri ciudate (cele marcate cu verde). Dacă folosim un identifier pe prima dintre ele, o să aflăm ca textul a fost criptat utilizând metoda denumită **ADFGX.** După asta ne dăm seama că celelalte două string-uri sunt pentru decriptarea primului (cel de-al doilea fiind **square grid-ul** pentru criptare, iar al doilea fiind **key-ul**).  
 După ce decriptăm, obținem string-ul **RHANRAENTPDNETTORASLDORDBISLEALANOTFTAOENTWIOOSERENFETTRIGOOEHRFCTHELLNUNLALRELMIRSEDPSHUYTTHDTREKEYDAIQ**, dar acesta nu este soluția probleme. Dacă inspectăm puțin mesajul, observăm că avem cuvântul **KEY**, ceea ce ne duce cu gândul că textul a fost criptat din nou. Folosindu-ne doar de această parte din string **RHANRAENTPDNETTORASLDORDBISLEALANOTFTAOENTWIOOSERENFETTRIGOOEHRFCTHELLNUNLALRELMIRSEDPSHUYTTHDTRE**, într-un identifier ni se indică că s-ar fi folosit **Transposition Cipher**, doar că atunci când încercăm să decriptăm mesajul cu cheia **DAIQ**, observăm că nu obținem nimic citibil. Aici intevine acel indiciu din descrierea problemei: „...part of the text was encrypted using the Vigenère cipher with the key "AXIS".” . Dacă decriptăm **DAIQ** folosind indiciul dat, o să avem un nou key: DDAY. Acuma, cu toate datele necesare, putem obține plaintext-ul **BERLINHASFALLENRETREATALLREMAININGTROOPSTODEFENDTHEPARTSOFTHECOUNTRYTHATWESTILLHOLDDONOTSURRENDER** atunci când ne folosim de un **Transportation Decipher**.

Sper că a fost fun challange-ul meu!  
GMC