Avsändare: Huvudkontoret avdelning TDDC75
Till: Speciella basgruppen
Kvalificerat hemlig, ej för vidare spridning

Ny information till det pågående uppdraget att avkoda IT-motståndarnas krypterade meddelanden.

De meddelanden som har uppsnappats av är krypterade med AES (CBC mode). Den interna IT-stödsavdelningen har bekräftat att tjänsten http://aes.online-domain-tools.com/ är tillförlitlig att använda till detta.

Antalet möjliga nycklar är $3,4*10^{38}$. Ni har redan hittat ett mönster som behöver upprepas tillräckligt många gånger för att få nyckeln.

Enda informationen som ni nu saknar är att hitta den så kallade initialiseringsvektorn. Denna vektor eller sträng kan uttryckas som $x_1x_2...x_{16}$, där varje x_i är ett ASCII-tecken. Vi vet följande:

- $\forall x_i : x_i \in \{A, B\}$
- $\exists x_i : x_i = A$
- $\forall x_i, x_{i+1} : (x_i = B) \rightarrow (x_{i+1} = B)$

Den krypterade texten (i hexkod) är:

dbca9f777720428c9876ac1291ad1392e7fd73e0051ef5944299967488e610e7dcefd6b5e
85af9a427a32c48a3132a26d454a264fda2c33184ec5873635e062cc2075b7dddd1063809
2915b77703d4257e870869b776ef3f0112e22fb7b6572f6025f46f53620b3faae8640f192
640c8d8430b135158a9772afcc2332d8657b21453a8dfd7b59458d052af29998d72fc2ce7
eeeb5789602952cc168c162da388e24940d7f8d1e11ffa5aaa9f0d8d46217c52f2832e033
1a836f39af46186426def8188166e18060b2333aa9ffe5bc3a25674042598fd7cb9de6b06
67d50b337a816cebde471b8b2b0eeacead949c009e9adea51fe0aacca5f88b50fb76fd078
ecbf8f5a5bb75652b0943c3d786bbcae9aa3095f2b3d62a572da0c322cf20b9f7be26e175
1e969e56651d9b8f69a4852f9d3a135f7ae464c920b034fe6ea19d71969bf5afa0b044be8
3634a7ee30d257962a28d3f0eefcc233a3d92f8dcf38cdfaa1195fbf1fa736ab4cb63c483
a731cf71c155dd1a0aeeb894e8f9a52832df5cd6c95e1dca43e8620cfe408002df4015ee7
a29aab9e167799c09c5c1083724f7f44a97656f6e2b9c2451dc3f8c751aca34b3a4b94ca5
e2a9613356557a4ceb032c5931ac308b8d7c097aae59bf1c21a167ede95ab165ab6bd5a1a
1bd1e9b3386