

Bezpieczne po??czenia?

Zmieniony 09.11.2013.

Wiadomo, ?e Ed Snowden co jaki? czas podaje nam gar?? ogólnych faktów na temat poufno?ci naszych E-maili, danych itd. Tym razem Snowden zaszokowa? wszystkich prawdziw? bomb?. Otó? standardowe programy do szyfrowania, (prawdopodobnie SSL) s? skopane ju? na etapie projektowania, ?eby NSA mog?o sobie poogl?da? conieco. W czym problem?

O ile dobrze mi wiadomo, algorytm AES jest standardem w dziedzinie algorytmów szyfrowania, przy którym majstrowa?o m in. NSA. Gdy wy?aniano algorytmy szyfruj?ce na zasadzie konkursu, szyfr Rijndael sta? si? standardem, ze wzgl?du na optymalne wywa?enie mi?dzy moc? szyfrowania, a szybko?ci?, Przegra? z nim ciut wolniejszy, otwarto?ród?owy Twofish, który podobno nie zosta? nigdy z?amany. Jako ?e AES jest standardem, ja osobi?cie postanowi?em u?ywa? do szyfrowania zarówno twofish jak i AES, Mo?e to co? pomo?e. Poza tym mo?liwe, ?e jak SSL jest skopany, nale?a?oby szyfrowa? dane jeszcze przed wysy?aniem czegokolwiek, co uniemozliwi/utrudni deszyfrowanie na etapie wysy?ki danych. Niestety, jak zwykle Snowden nie podaje jakichkolwiek szczegó?ów, a mówi ogólnikami, wi?c w?a?ciwie nie wiadaomo, jak temu przeciwdzia?a?, lub chocia?by utrudnia? dla NSA zadanie.

Jedynie co pozosta?o na pocieszenie, to to, ?e USA na szcz??cie nie s? skore do wspó? pracy z byle kim, wi?c np polskie s?u?by specjalne mog? sobie conajwy?ej poprosi? o rozkodowanie czego?tam i najcz?sciej dosta? odpowied? odmown? odno?nie dalszego przekazanie informacji.