

Re: Weak keys for ElGamal

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2006-10/msg00859.html>

- *From:* daw@xxxxxxxxxxxxxxxxxxxxxxxxxxxx (David Wagner)
 - *Date:* Fri, 27 Oct 2006 22:37:45 +0000 (UTC)
-

Anton Berg wrote:

let's consider the typical ElGamal encryption with primes $p=2q+1$. Let g be a generator of the q -order group G for which the DL assumption holds. The secret key x is from $\{1, \dots, q-1\}$ and messages are taken from G . If in general the discrete logarithm problem is hard in G are there any weak keys from $\{1, \dots, q-1\}$?

The very notion of "weak keys" makes no sense, given modern understanding of confidentiality. Security in crypto is inherently a probabilistic notion: what are the chances that an adversary guesses the message? (You can never make that probability exactly zero.)

So could a party by chance (or intentionally) choose a weak secret key and thereby reduce the security of the ElGamal scheme?

Those are two different questions.

If one of the parties is malicious, they can just reveal the message or key, so it doesn't make sense to ask for El Gamal to be secure if one of the parties is malicious.

As for choosing a weak key by chance, the best way to answer the question is to unask the question and ask a different one, because weak keys are not a very relevant concept.

Are there any efficient algorithms to compute the DL but which can only be applied if the secret key x satisfies somehow "special conditions"?

Sure. If I know that $x=42$, then I have a very efficient algorithm for computing x (i.e., computing the discrete log)! See how silly these questions can become?

Re: Weak keys for ElGamal

I am sure, that this is not possible because the computation of the discrete logarithm is random-self-reducible. Am I right with my suggestion?

Yes, it is random-self-reducible.