A Controversial Key-Agreement Protocol

Frozen Maize

Abstract

Suppressed from publication for several years, we present an interesting key agreement protocol, called CRAP (short for *Controversial Rey-Agreement Protocol*). We highlight some useful results pertaining to the security of this CRAP, that were previously unknown to the participants that were using this scheme.

1 Introduction

The beauty of manipulating algebraic equations has led to many, many, many new cryptographic protocols, as well as providing an opportunity to practise using LaTeX.

In this paper, we present an interesting key agreement protocol, called CRAP (short for *Controversial Rey-Agreement Protocol*)[1]. This CRAP was initally drafted in 1998 by the author (codenamed "anonymous"), who was a PhD student at the time, and it was shown to a small group of cryptology researchers (who might now recognise its sudden appearance in the craptologic literature).

Politics and cryptology are sometimes a controversial combination, and this protocol is no exception. It is due to the controversial nature of the result that this paper was supressed from earlier publication, by the author, but he now feels that the sudden re-emergence of interest in craptology warranted submission.

There! That should be enough padding to make this paper appear legitimate. Now we proceed with a detailed description of the CRAP.

2 The Protocol

Alice and Bob want to agree a secret key K for a symmetric-key cipher over an insecure channel. Assume Alice and Bob share a public prime modulus n.

1. Alice chooses a prime number p $(p < n)$ and sends p to Bob. Note that $p \in \mathbb{Z}_n^*$, the multiplicative group of integers mod n.

2. Bob chooses a number q that is relatively prime to $\phi(p) = (p - 1)$ and sends $B = pq \pmod{n}$ to Alice.

[1] For people who are unfamiliar with the terminology differences between cryptology and craptology, we define the term "rey" to mean: key.

3. Alice computes $A = p^{-1}B \pmod{n}$, and sends A to Bob.

4. Alice and Bob each calculate the shared secret key $K = (A + B)$.

At a glance this protocol appears to be flawed in that an evesdropper may determine the secret key K from observation of A and B. However, neither Alice nor Bob were aware of this and that is why when Bob got home and went to sleep, his evesdropping wife Bobbitt cut off his tool[2] [2, 3, 4, 5].

3 Disclaimer

Any resemblence to actual persons, living or dead, is unintentional. Events similar to the one in this paper have happened, so we end this paper with the moral of this story:

As Julius Caesar, inventor of the first craptographic block cipher [6], might have said: "Caveat, you cheating scoundrel!" (if he could speak English and couldn't find the complete Latin translation of what he intended to say).

References

[1] Diffie Hellman, "A key agreement protocol", private communication, 1970's.

[2] Bob, "Meeting tonight", not-so-private communication, 1990's.

[3] Alice, "Re: Meeting tonight", not-so-private communication, 1990's.

[4] Bob, "How was last night for you?", not-so-private communication, 1990's.

[5] Alice, "It was okay", not-so-private communication, 1990's.

[6] Julius Caesar, "A block cipher with a 4.7-bit key", Proceedings of *First International Workshop on Fast Paper-And-Pencil Encryption*, Lecture Notes in Abacus Science, to appear[3].

[2] ...and flushed it down the toilet.

[3] ...assuming that someone actually discovers the existance of this historical paper.