New directions in cryptography (volume II) (Preliminary Daft)

Lars R. Knudsen

November 13, 2000

Abstract

There is a folklore theorem which says that public-key cryptosystems are more secure than conventional, secret-key cryptosystems. However, this is not true. In this paper it is shown that a modification of the Data Encryption Standard is at least as secure as the RSA cryptosystem, if not more. We think this is a milestone result in modern cryptography which will have worldwide implications.

Keywords. Definitely Craptology.

1 Introduction

I was born in Denmark in 1962...

2 The RSA cryptosystem

The RSA cryptosystem [3] is one of the most popular cryptosystems in the world today. RSA stands for Rock Solid Algorithm, and it was invented many years ago in the USA.

In RSA one chooses two k-bit primes p and q, forms the modulus $n = pq$ and chooses an encryption key e and a decryption key d such that $ed = 1 \bmod (p-1)(q-1)$. Encryption of a cleartext x is then $y = x^e \bmod n$. Decryption of $y = x^e \bmod n$ is $y^d \bmod n = x$. Recently a 512-bit version of RSA was broken in a dutch treat. Therefore it is often recommended to use moduli of at least 768 bits.

The following two results are essentially the only security results known about the RSA cryptosystem.

Theorem 1 *Let $n = pq$ be an RSA-modulus. If n can be factored, then the RSA cryptosystem can be broken.*

Proof: If you can factor n, then you also know p and q, which is easy to show. But then since $ed = 1 \bmod (p-1)(q-1)$ one gets that $ed-1 = k(p-1)(q-1)$ for some unknown k. Now one guesses k and computes $ed = k(p-1)(q-1)+1$ from which d can be found if e is known. When d is known one can decrypt any ciphertext. Since e is known one can also encrypt any plaintext, but you can always do that. ■

Theorem 2 *Let $n = pq$ be an RSA-modulus. If the decryption exponent d can be found, then n can be factored.*

Proof: As before one knows that $ed = k(p-1)(q-1)+1$. Since k is known already, see proof of Theorem 1, one can compute $(ed-1)/k = (p-1)(q-1)$ from which p and q can be extracted. ■

3 The DES cryptosystem

The DES [2] is the most studied and well-known cryptosystem today. It was invented even earlier than the RSA cryptosystem and designed to resist also unknown attacks. Many people were involved in the design of the DES but nobody is really sure who invented what, and those who can remember do not want to tell.

The DES encrypts a 64-bit cleartext to a 64-bit ciphertext using a 56-bit user selected key. The cipher runs in 16 rounds, each round uses a subkey of 48 bits, in total 768 subkey bits. These bits are derived from the user selected 56 bits in the key schedule. For more details we refer to almost any book on cryptography.

3.1 The DES' cryptosystem

At Crypto'82 Tom Berson [1] suggested to choose the 768 subkey bits of the DES independently instead of generating them from a small 56-bit key. Tom is a wise man, and we always try to do what he recommends. The DES' cryptosystem is the same as the DES cryptosystem except for the key schedule, which is as follows. First we choose two 384-bit primes p and q, just as we would choose them in a 768-bit RSA cryptosystem. We split p into eight blocks of each 48 bits, which make the first eight DES' subkeys. Then we split q into eight blocks of each 48 bits, which make the last eight

DES' subkeys. Voilà, DES'. Two parties which share p and q can clearly encrypt and decrypt as in any conventional scenario using the DES. For DES' if the users also publish the value of $n = pq$, then we can prove the following security results for DES'. The proofs of these theorems will follow in the full version of this paper.

Theorem 3 *Let $n = pq$ where p and q are the two halves of a DES'-key. If n can be factored, the DES' cryptosystem can be broken.*

Theorem 4 *Let $n = pq$ where p and q are the two halves of a DES'-key. If the decryption key of DES' can be found, then n can be factored.*

It follows that these two results of security for the DES' cryptosystem match exactly the above two results of security for the RSA cryptosystem, and thus we conclude that

> the DES' cryptosystem is **as secure as** the RSA cryptosystem.

Note that it is essential for the proof of security of DES' that the value of n is published. One could think that n can stay secret along with p and q and thus conclude that the DES' cryptosystem is **more secure than** the RSA cryptosystem. However, we were not able to prove this because the air-conditioning system on our Turing machine is currently not working.

References

[1] T. A. Berson. Long key variants of DES. In David Chaum, Ronald L. Rivest, and Alan T. Sherman, editors, *Advances in Cryptology: Proceedings of Crypto '82*, pages 311–314, New York, USA, 1982. Plenum Publishing.

[2] National Bureau of Standards. Data encryption standard. Federal Information Processing Standard (FIPS), Publication 46, National Bureau of Standards, U.S. Department of Commerce, Washington D.C., January 1977.

[3] R. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystem. *Communications of the ACM*, 21(2):120–126, 1978.