## 1 Forging X.509 Certificates

We consider X.509 certificates signed by using the `md5WithRSAEncryption`. We want to submit an RSA public key $(N_1, e_1)$ to the certificate authority for certification such that we can infer a fake certificate for another RSA public key $(N_2, e_2)$. RSA moduli are assumed to be 2048-bit long. We also assume that $e_1 = e_2 = 65537$ and that all fields except the moduli parts in both certificates will be completely identical.

We assume that we have filled all fields of the X.509 form, except the RSA modulus part (and the signature to be appended by the certificate authority). We assume that the length of the form (represented as a string) from the beginning of the form to the beginning of the modulus field is a multiple of 512 bits.

1. Preliminaries.
   We recall the Merkle-Damgård scheme for the MD5 hash function. MD5 is an iterative hash function which proceeds by first padding the message with a string which only depends on its length so that the padded string has a length multiple of 512 bits, then splitting it in a sequence of 512-bit blocks. Every block is then iteratively hashed by using a compression function $C$. More precisely, we define a sequence $H$ by $H_0 = \mathsf{IV}$ where IV is a standard initial vector and $H_i = C(H_{i-1}, X_i)$ where $X_i$ is the $i$th block to be hashed. The last $H_i$ value is the hash of the message.
   (a) We denote by $\mathsf{MD5}'$ the hash function obtained from MD5 by removing the padding scheme and replacing the standard initial vector IV by an arbitrary 128-bit string $\mathsf{IV}'$. Show that there exists a vector $\mathsf{IV}'$ such that for any $N_1$ and $N_2$ such that $\mathsf{MD5}'(N_1) = \mathsf{MD5}'(N_2)$, the strings to be signed in both certificates produce identical MD5 hash values.
   (b) We recall that strings are signed using `md5WithRSAEncryption` by first hashing by using MD5, then putting the hash in a specific format, and finally signing by using the plain RSA signature scheme.
   With the above $\mathsf{IV}'$ and $\mathsf{MD5}'$, deduce that if $\mathsf{MD5}'(N_1) = \mathsf{MD5}'(N_2)$, a valid signature for the certificate with $N_1$ is also a valid signature for the certificate with $N_2$.
   (c) We assume that we can find two different 1024-bit blocks $b_1$ and $b_2$ such that $\mathsf{MD5}'(b_1) = \mathsf{MD5}'(b_2)$. (We actually can, very efficiently!)
   Show that for any 1024-bit string $b$, we have $\mathsf{MD5}'(b_1||b) = \mathsf{MD5}'(b_2||b)$.
2. Constructing $N_1$ and $N_2$.
   By using the previous notations, it remains to find $b$ such that $N_1 = b_1||b$ and $N_2 = b_2||b$ are valid RSA moduli for which we know the factorization.
   (a) We recall that a valid RSA modulus is a product of two different large prime integers. Let $p_1$ and $p_2$ be two (different) random 512-bit prime numbers. Show that we can compute and integer $b_0$ between 0 and $p_1p_2$ by using the Chinese Remainder Theorem such that $p_1$ divides $b_1 2^{1024} + b_0$ and $p_2$ divides $b_2 2^{1024} + b_0$.
   (b) By taking $b = b_0 + kp_1p_2$ for $k = 0, 1, 2, \ldots$, (heuristically) show that we are likely to find $k$ such that $(b_1 2^{1024} + b)/p_1$ and $(b_2 2^{1024} + b)/p_2$ are both primes. Conclude.
3. Discussion.
   (a) To what extend is the above attack devastating?
   (b) We now assume that given two vectors $\mathsf{IV}'$ and $\mathsf{IV}''$ defining $\mathsf{MD5}'$ and $\mathsf{MD5}''$ we can find two 1024-bit blocks $b_1$ and $b_2$ such that $\mathsf{MD5}'(b_1) = \mathsf{MD5}''(b_2)$. Can we now derive a more dangerous attack?
   (c) We now assume that given a vector $\mathsf{IV}'$ defining $\mathsf{MD5}'$ and a 1024-bit block $b_1$ we can find another 1024-bit block $b_2$ such that $\mathsf{MD5}'(b_1) = \mathsf{MD5}'(b_2)$. Can we now derive an even more dangerous attack?

## 2 Solution

1. Preliminaries.
   (a) The filled part of the certificate consists of an integral sequence of 512-bit blocks $X_1, \ldots, X_i$. By appending the RSA modulus $N_j$ we have two new blocks such that $X^j_{i+1}||X^j_{i+2} = N_j$. By taking $\mathsf{IV}' = H_i$, we have $\mathsf{MD5}'(N_j) = H^j_{i+2}$, so $\mathsf{MD5}'(N_1) = \mathsf{MD5}'(N_2)$ is equivalent to $H^1_{i+2} = H^2_{i+2}$. The remaining part of the filled (padded) certificate appends a final sequence of constant blocks.
   (b) Since the signature only depends on the hashed value, a collision on the hash function makes a valid signature on the first message be a valid signature for the second message.

   (c) By iteratively hashing the 2-block sequence $b_1$ or $b_2$, if we already have a collision on $H_2$, then we continue to have collisions if we iteratively hash the same sequence of blocks.

2. Constructing $N_1$ and $N_2$.
   (a) Since $p_1$ and $p_2$ are different, they are coprime. Hence, from the Chinese remainder theorem, for any $x_1 = -b_1 2^{1024}$ and any $x_2 = -b_2 2^{1024}$, we can find $b_0$ between 0 and $p_1 p_2$ such that $b_0 \equiv x_1 \pmod{p_1}$ and $b_0 \equiv x_2 \pmod{p_2}$. We deduce that $p_1$ divides $b_1 2^{1024} + b_0$ and that $p_2$ divides $b_2 2^{1024} + b_0$.
   (b) Assuming that $b = b_0 + kp_1 p_2$ looks like a random integer, we can further assume that $(b_1 2^{1024} + b)/p_1$ and $(b_2 2^{1024} + b)/p_2$ also look like random independent integers. Eventually, both will be prime. We obtain $q_1 = (b_1 2^{1024} + b)/p_1$ and $q_2 = (b_2 2^{1024} + b)/p_2$ so $b_1 || b$ and $b_2 || b$ are two RSA moduli $N_1$ and $N_2$ with factorization $N_1 = p_1 q_1$ and $N_2 = p_2 q_2$.

3. Discussion.
   (a) This attack produces certificates with all fields (except the RSA modulus) in common. So this does not really forge a certificate for an entity which is unknown by the certificate authority. It is just weird that the authority does not see the right public key it is signing. The attack is not so devastating.
   (b) If we knew how to make collisions with two different arbitrary initial vectors, we could have changed the fields before the modulus part. This could be much more devastating: we could request a certificate for a fake company and transform it into a valid certificate for another one with another public key.
   (c) If we knew how to make second preimage attacks, we could use an existing valid certificate from a company and change its public key. This would be a disaster for the public key infrastructure.

This exercise was inspired by the memo “Colliding X.509 Certificates” by Arjen Lenstra, Xiaoyun Wang, and Benne de Weger version 1.0 from 1.3.2005:

http://eprint.iacr.org/2005/067