COMPOSITE DIFFIE-HELLMAN PUBLIC-KEY
GENERATING SYSTEMS ARE HARD TO BREAK

by
ZAHAVA SHMIDLY

Technical Report # 356
February 1985

TECHNION - ISRAEL INSTITUTE OF TECHNOLOGY
DEPARTMENT OF COMPUTER SCIENCE
HAIFA, ISRAEL
COMPOSITE DIFFIE-HELLMAN PUBLIC-KEY
GENERATING SYSTEMS ARE HARD TO BREAK

by
ZAHAVA SHMUELY

Technical Report # 356

February 1985
COMPOSITE DIFFIE-HELLEMAN PUBLIC-KEY
GENERATING SYSTEMS ARE HARD TO BREAK

by

Zahava Shmuely

ABSTRACT

The use of a large composite modulus \( n = pq \) in the Diffie-Hellman
public-key generating system instead of the originally proposed prime
modulus \( p \) [1] is suggested. It is shown that cracking the modified
(composite) system obtained is at least as hard as the factorization of \( n \).

The composite Diffie-Hellman system thus appears to enjoy the
combined cryptographic benefits of both (believed to be hard) problems:
(i) factorization of a large composite number \( n = pq \) where \( p, q \) are
primes, (ii) finding the discrete logarithms both modulo \( p \) and modulo \( q \).

It is also shown that the cracking problem for Mental Poker Playing
as suggested by Shamir, Rivest and Adleman [2] is similar to that of
cracking the composite Diffie-Hellman system described above. Consequently,
cracking Mental Poker Playing is at least as hard as the factorization
of the composite modulus \( n \) used when playing.
INTRODUCTION

In this paper we investigate a composite version of Diffie and
Hellman's original public-key generating system, see [1]. Here the
publicly known modulus \( \mathbf{n} = pq \) where \( p, q \) are large secret prime numbers,
and base \( a, 1 < a < n \), are used to generate encryption keys as follows.
Each user \( A_i \) chooses a secret key \( 0 < x_i < n \) and uses it to get his
public key \( K_i = a^{x_i} \pmod n \). Any pair of users \( A_i, A_j \) may use the
publicly known keys

\[
(1) \quad K_i = a^{x_i} \pmod n, \quad K_j = a^{x_j} \pmod n, \\
\quad \text{in order to simultaneously generate a common secret key,}
\]

\[
(2) \quad K_{ij} = a^{x_i x_j} \equiv K_i x_j \equiv K_j x_i \pmod n.
\]

Note that in the original Diffie-Hellman system the public modulus was
chosen to be a prime number \( p \). In the suggested composite system the
public modulus \( n \) is known to be composite and its secret factors \( p, q \)
are not needed when using the system as in (1) or (2) above.

We prove here that finding \( K_{ij} \) by using only the public information
\( I_i = \{n, a, K_i, K_j\} \) is at least as hard as factoring \( n \). This is
done by showing that any algorithm \( \mathcal{A} \) which cracks the system for a
can be used to extract quadratic roots modulo \( n \) (see [3]) in \( O\left(2^{k+1} \cdot 2^{l+1}\right) \)
steps where \( k = \frac{\tau}{2}(p-1), \quad l = \frac{\tau}{2}(q-1) \) resp. denote the highest powers
of 2 dividing \( p-1, q-1 \) resp.
The set \( \mathcal{Q}(n) \) itself is characterized and shown to contain \( \frac{1}{2} \cdot \mathbf{n} \)
of all elements relatively prime to \( n \). The cryptographic strength of the
Diffie-Hellman composite system is further demonstrated by proving
that a Diffie-Hellman cracking algorithms AL can be used to crack RSA-encrypted messages (see [4]) even when the elements of $Q(n)$ are not accepted as admissible base elements for AL.

More generally, suppose that a common symmetric secret key $K_{12\ldots s}$ is simultaneously generated by a group of $s > 2$ users $A_i$, $1 \leq i \leq s$, each having a secret key $x_i$, in the following way: at the $r$-th stage, $1 \leq r \leq s-1$, all the $s_r = \binom{s}{r}$ common "partial" keys $x_{i_1}x_{i_2}\ldots x_{i_r} \equiv a^{j_1j_2\ldots j_r} \pmod{n}$ are made public by the corresponding members of the $r$-element groups $\{A_{j_1}, A_{j_2}, \ldots, A_{j_r}\}$. Each user $j_r$ is then able to compute for himself all the $\binom{s-1}{r-1}$ group keys for those $r+1$-element groups to which he belongs

$$K_{12\ldots j_1j_2\ldots j_{r+1}} = x_{i_1}x_{i_2}\ldots x_{i_r} \equiv a^{j_1j_2\ldots j_{r+1}} \pmod{n}$$

If $r+1 < s$ the process is repeated with $r$ replaced by $r+1$. Otherwise each user holds the common secret key

$$K_{12\ldots s} = a^{x_1x_2\ldots x_s} \pmod{n}.$$ 

Clearly, the basic composite Diffie-Hellman system is defined for the case $s = 2$.

It is shown that finding the common key $K_{12\ldots s}$ by using all partial public information $I_{s-1} = \{n, a, K_{12\ldots i_2}\ldots i_r \equiv a^{x_{i_1}x_{i_2}\ldots x_{i_r}} \pmod{n}\}$ for all $\binom{s}{r}$ possible choices of indices $1 \leq i_1 < i_2 < \ldots < i_r \leq s$ where $1 \leq r \leq s-1$ is at least as hard as factoring $n$.

Thus, the user $A_i$ may change periodically his public key from

$$K_i^{j} \rightarrow K_i^{j+1} \equiv (K_i^{j})^{x_i} \pmod{n}$$

without weakening the system.
As another possible use we mention the safe generation of common keys or cryptographically strong sequences $K_n = \alpha^m \pmod{n}$, $n = 1, 2, \ldots$, within a group of users sharing a common secret seed $\alpha$. It should be emphasized that for the different ways of using the system suggested here there is no need to know the secret factorization of $n$.

The results obtained here indicate that the composite Diffie-Hellman (generalized) Public-Key generating system seems to have certain advantages. To these we also add the following observation. The problem of finding the secret key $x_i$ by using the public information

$I_0 = \{n, \alpha, K_i \equiv \alpha^x \pmod{n}\}$

is at least as hard to crack as each of the following two problems (in fact it is equivalent to the solution of both): (i) FACT: finding the prime factors $p, q$ of $n$ (see [5])

(ii) DLOG: finding discrete logarithms in both Galois fields $GF(p)$, $GF(q)$.

Thus composite Diffie-Hellman systems enjoy the combined cryptographic strength of these two believed to be hard number-theoretic problems.

Mental Poker Playing, a method for passing secret messages between two partners $A$ and $B$ was suggested in [2]. Here both partners choose a common (public) composite key $n = pq$ while keeping the prime factors $p, q$ secret. To pass a message $1 < m < n$ from $A$ to $B$, $A$ picks a random number $1 < x < n$, $(x, \phi(n)) = 1$ and sends $m^x \pmod{n}$ to $B$. $B$ adds his encryption to the message by similarly choosing $1 < y < n$, $(y, \phi(n)) = 1$ and sending back $(m^x)^y \pmod{n}$. Now $A$ makes use of the secret decomposition of $n$ to find $x^*$, the multiplicative inverse of $x$ modulo $\phi(n)$, and sends to $B$ the message $(m^{xy})^x \equiv m^y \pmod{n}$. By similarly finding $y^*$, $B$ finally gets the secret message

$(m^y)^x \equiv m \pmod{n}$. 
Here we show that the problem of cracking Mental Poker Playing, i.e., finding the message \( m \) when given the public information
\[
I_1 = [n, m^x, m^y, m^y \text{ (mod } n)]
\]
is just a particular case of cracking the composite Diffie-Hellman public key generating system. It follows that cracking Mental Poker Playing is at least as hard as the factorization of the composite modulus \( n \) used by the players.

2. PRELIMINARIES

It is well known, see e.g. [6], that the large prime factors \( p, q \) of a hard to factor composite number \( n = pq \) must satisfy

\[(4) \quad p-1 = \epsilon p', \quad q-1 = \delta q'
\]

where both \( p', q' \) are large prime numbers. Here \( \epsilon, \delta \) are assumed to be relatively small. Put \( r = \#_2(s) \) when \( 2^r | s, \ 2^{r+1} | s \). For the primes \( p, q \) satisfying (4) we put

\[(5) \quad k = \#_2(p-1), \quad \ell = \#_2(q-1).
\]

where \( \ell, k \geq 1 \). We also let

\[(6) \quad \hat{p} = \frac{p-1}{2^k} = \epsilon \cdot p', \quad \hat{q} = \frac{q-1}{2^\delta} = \delta \cdot q'.
\]

denote the odd parts of \( p-1, q-1 \) respectively. Obviously, \( 2^k | \epsilon \),
\( 2^\delta | \delta \) and \( (p-1, q-1) = (\ell, \delta) \geq 2 \). From now on \( n = pq \) is always assumed to satisfy (4) and the notations (5), (6), will be freely used.

For any number \( m, \ Z_m^* = \{a | 1 \leq a \leq m, (a, m) = 1 \} \) is the multiplicative group modulo \( m \) where \( (a, m) \) stands for the gcd of \( a \) and \( m \).

\( \phi(m) = |Z_m^*| \), the number of elements in \( Z_m^* \), is the Euler totient of \( m \) [7]. For any \( 1 \leq j \leq n \) satisfying \( (j, \phi(n)) = 1 \) let \( j^* \) denote the multiplicative inverse of \( j \) modulo \( \phi(n) \). As is well known
\( e^{jx} \equiv a \pmod{n} \) holds for all \( 1 \leq a \leq n \). When \((j, n) = 1\) we let \( j^{-1} \) denote the multiplicative inverse of \( j \) modulo \( n \). For any \( a \in \mathbb{Z}_n^* \), put

\[
(7) \quad B(a) = \{b | b \equiv a^x \pmod{n} \text{ for some } 1 \leq x \leq n\}
\]

and

\[
(8) \quad C(a) = \{b | b \equiv a^x \pmod{n} \text{ for some } 1 \leq x \leq n \text{ satisfying } (x, 4(n)) = 1\}.
\]

Clearly, \( C(a) \subseteq B(a) \), Also when \( \hat{a} \in C(a) \) then \( C(\hat{a}) = C(a) \). In the following we will be interested in the number of different representations

\[
a^x \equiv b \pmod{n}, \quad 1 \leq x \leq (p-1)(q-1)
\]

for a fixed \( b \in B(a) \). To do this let \( g, h \) respectively denote generators of the cyclic groups \( \mathbb{Z}_p^*, \mathbb{Z}_q^* \).

By the Chinese Remainder Theorem (see [7]), each \( a \in \mathbb{Z}_n^* \) can be uniquely represented by

\[
(9) \quad a = g^a \pmod{p}, \quad b = h^b \pmod{q}, \quad 1 \leq a \leq p-1, \quad 1 \leq b \leq q-1.
\]

Now let

\[
(10) \quad \xi_1 = \xi_1(a) = (a, p-1), \quad \xi_2 = \xi_2(a) = (b, q-1).
\]

Both \( \xi_1 = \xi_1(a) \), \( \xi_2 = \xi_2(a) \) do not depend on the particular choice of the generators \( g, h \) (see [7]). It follows easily that

\[
C(a) = \{\hat{a} | \xi_1(\hat{a}) = \xi_1(a), \quad \xi_2(\hat{a}) = \xi_2(a)\} \quad \text{while} \quad B(a) = \cup\{C(\hat{a}) | \xi_1(\hat{a}) = \xi_1(a), \quad \xi_2(\hat{a}) = \xi_2(a)\}.
\]

For \( a \in \mathbb{Z}_n^* \) satisfying (9), (10), we may put \( a = \xi_1(\hat{a}), \quad b = \xi_2(\hat{b}) \)

where \( (\xi_1, \frac{p-1}{\xi_1}, \xi_2, \frac{q-1}{\xi_2}) = 1 \). The following is easily proved.

Lemma 1: Let \( b \in B(a) \) for some \( a \in \mathbb{Z}_n^* \) satisfying (9). Then

\[
b \equiv a^x \pmod{n}
\]

for some integer \( x \) iff
(11) $x_1 \equiv x_0 \pmod{M}$ where $M = \text{lcm}(\frac{p-1}{\xi_1}, \frac{q-1}{\xi_2}) = \frac{(p-1)(q-1)}{\xi_1 \xi_2}$

for $\xi_1 = \xi_1(a)$, $\xi_2 = \xi_2(a)$ given in (10).

It follows that for each $b \in B(a)$ there exist $\xi_1 \xi_2(\frac{p-1}{\xi_1}, \frac{q-1}{\xi_2})$ elements $1 \leq x_1 \leq (p-1)(q-1)$ satisfying $a^{x_1} \equiv b \pmod{n}$. Thus

$$|B(a)| = \{b \equiv a^x \pmod{n}\} = M = \frac{(p-1)(q-1)}{\xi_1 \xi_2} \left(\frac{p-1}{\xi_1}, \frac{q-1}{\xi_2}\right).$$

If in particular $\xi_1 = \xi_1(a)|\epsilon$, $\xi_2 = \xi_2(a)|\delta$ where $\epsilon$, $\delta$ are given in (4) (which happens for at least $(1 - \frac{1}{p'})(1 - \frac{1}{q'})$ of all $a \in \mathbb{Z}^*_n$) then

$$|B(a)| > \frac{(p-1)(q-1)}{\epsilon \delta (\epsilon, \delta)} = \frac{p'q'}{(\epsilon, \delta)}.$$ 

We also use the following lemma. See the Appendix for the proof.

**Lemma 2:** Let $b \equiv a^x \pmod{n} \in B(a)$ where $a \in \mathbb{Z}^*_n$ and let $1 \leq e \leq n$ be given where $(e, \phi(n)) = 1$. Then $(x, e) = 1$ holds for $\frac{\phi(e)}{e}$ of all elements $x_i$ satisfying $a^{x_i} \equiv b \pmod{n}$.

A central role here is played by the set

(12) $Q(n) = \{a \in \mathbb{Z}^*_n \mid a^{2t} \equiv t \pmod{n} \text{ for some } t\}.$

The following theorem characterizes $Q(n)$. The proof is given in the Appendix.

**Theorem 3:** Let $a \in \mathbb{Z}^*_n$ satisfy

$$a \equiv g^a \pmod{p}, \ a \equiv h^\beta \pmod{q}, \ 1 \leq a \leq p-1, \ 1 \leq \beta \leq q-1$$

where $g$, $h$ are cyclic generators of $\mathbb{Z}^*_p$, $\mathbb{Z}^*_q$ respectively.
Then the following are equivalent:

(i) \( a \in \mathbb{Q}(n) \); (ii) \( a \equiv a^{-1} \pmod{n} \) where \( (t_1, \phi(n)) = 1 \);

(iii) \( a^2 \equiv a^5 \pmod{n} \) where \( a \) is an odd number; (iv) \( a^2 \equiv a^{s_1} \pmod{n} \) where \( (s_1, \phi(n)) = 1 \);

(v) \( 2^k | a, 2^\ell | b \) where \( k = \#_2(p-1), \ell = \#_2(q-1) \).

Letting \( \hat{p} = \frac{p-1}{2^k}, \hat{q} = \frac{q-1}{2^\ell} \) we find that a universal invertible exponent \( t_1 \) for all the elements \( a \in \mathbb{Q}(n) \) w.r.t. (ii), Theorem 3 is given by

\[
(13) \quad t_1 = \begin{cases} 
1/2 \cdot (1 + \frac{\hat{p} \cdot \hat{q}}{\hat{p} + \hat{q}}) & \text{when } \frac{\hat{p} \cdot \hat{q}}{\hat{p} + \hat{q}} \equiv 1 \pmod{4} \\
1/2 \cdot (1 + \frac{3\hat{p} \cdot \hat{q}}{\hat{p} + \hat{q}}) & \text{when } \frac{\hat{p} \cdot \hat{q}}{\hat{p} + \hat{q}} \equiv 3 \pmod{4} 
\end{cases}
\]

Similarly \( s_1 = \frac{\hat{p} \cdot \hat{q}}{\hat{p} + \hat{q}} + 2 \) is a universal exponent for \( \mathbb{Q}(n) \) w.r.t. (iv), Theorem 3, i.e., \( a^2 \equiv a^{s_1} \pmod{n} \) holds for all \( a \in \mathbb{Q}(n) \).

Theorem 3, (v) together with the uniqueness of representation in (9) and the fact that \( n \) is hard to factor (see (4), (5), (6)) yield

**Corollary 4:** A randomly chosen element \( a \in \mathbb{Z}_n^* \) belongs to \( \mathbb{Q}(n) \) with probability \( \frac{1}{2} \frac{k+\ell}{k+\ell} \) where

\[
\frac{1}{2} \frac{k+\ell}{k+\ell} \geq \frac{1}{c+\ell} = \frac{(p-1)(q-1)}{p'q'} \approx \frac{pq}{p'q'}. \]

\( \square \)
3. THE ALGORITHM AL

The composite Diffie-Hellman public key generating system was introduced in §1. Let AL denote an algorithm which cracks this system by using the public information $I_1 = \{n, a, a^X, a^Y\}$ only, that is,

$$\text{(14)} \quad \text{AL}(n, a, a^X(\text{mod } n), a^Y(\text{mod } n)) = a^{XY}(\text{mod } n).$$

Here $n, a, 1 \leq a^X(\text{mod } n) < n, 1 \leq a^Y(\text{mod } n) < n,$ are the input data fed into the algorithm while $1 \leq a^{XY}(\text{mod } n) < n$ is its output. Assuming form now on that $n$ is fixed we write (14) in the abbreviated form

$$\text{(14)°} \quad \text{AL}(a, a^X(\text{mod } n), a^Y(\text{mod } n)) = a^{XY}(\text{mod } n).$$

To show that AL is well-defined we state

**Lemma 5:** If $a = a^X(\text{mod } n), a = a^Y(\text{mod } n)$ then

$$a^{XY}(\text{mod } n) = a^{x_1y_1}(\text{mod } n).$$

**Proof:** $a^x = (a^x) = (a^x)^1 = a^{x_1y_1}(\text{mod } n).$ $\Box$

Concerning the algorithm AL we now make

**Definition 6:** Call $a \in \mathbb{Z}_n^*$ a $\left(\frac{1}{f_1}, \frac{1}{f_2}\right)-$admissible (respectively $\left(\frac{1}{f_1}, \frac{1}{f_2}\right)-C$-admissible) base element for the algorithm AL given in (14)* if AL outputs $a^{XY}(\text{mod } n)$ for at least $\frac{1}{f_1}$ of all inputs $a^X(\text{mod } n) \in B(a)$ (resp. $C(a)$) and at least $\frac{1}{f_2}$ of all inputs $a^Y(\text{mod } n) \in B(a)$ (resp. $C(a)$) fed into it. We say that the algorithm AL is $\left(\frac{1}{f_0}, \frac{1}{f_1}, \frac{1}{f_2}\right)-$admissible (resp. $-C$-admissible) if at least $\frac{1}{f_0}$ of all $a \in \mathbb{Z}_n^*$ are $\left(\frac{1}{f_1}, \frac{1}{f_2}\right)-$admissible (resp. $-C$-admissible).

An input triple $(a, a^X(\text{mod } n), a^Y(\text{mod } n))$ for which $a^{XY}(\text{mod } n)$ is output by AL is said to be proper for AL.
We note the following basic properties of $\text{AL}$ assuming that all input triples given below are proper for $\text{AL}$.

\[(15) \quad \text{AL}(a, a^x \pmod{n}, b) = b^x \pmod{n} \]

More generally, we have

\[(16) \quad \text{AL}(a^x \pmod{n}, a^y \pmod{n}, a^z \pmod{n}) = a^{xyz} \equiv j \pmod{n} \]

provided that $a^{x^z} \equiv a \pmod{n}$ holds for some $1 \leq x \leq n$. To show (16) write $a^y = (a^x)^{xy} \pmod{n}$, $a^z = (a^x)^{xz} \pmod{n}$ and use the definition of $\text{AL}$ to get $j = (a^x)^{xyz} = a^{xyz} \pmod{n}$ as stated. In particular, when $(x, \phi(n)) = 1$ then obviously

\[(17) \quad \text{AL}(a^x \pmod{n}, a^y \pmod{n}, a^z \pmod{n}) = a^{x^y z} \pmod{n} \]

4. THE ALGORITHM $AM$

Mental Poker Playing was described in the Introduction.

We now let $AM$ denote an algorithm which cracks Mental Poker Playing by using the publicly known information only. Thus, we have

\[(18) \quad AM(n, m^{xy} \pmod{n}, m^y \pmod{n}, m^x \pmod{n}) = m, \]

\[(x, \phi(n)) = (y, \phi(n)) = 1 \]

Again, the rightmost $n$ in (18) will usually be omitted. If we now set $a = m^{xy} \pmod{n}$ and use the fact that both $x, y$ are invertible modulo $\phi(n)$ we get $m^y = a^x \pmod{n}$, $m^x = a^y \pmod{n}$ and $m = a^{xy} \pmod{n}$. Substituting these into (18) and letting $x_1 = x^*$, $y_1 = y^*$, we get

\[(19) \quad AM(a, a^{-1} \pmod{n}, a^{x_1} \pmod{n}) = a^{x_1 y_1} \pmod{n}, \]

\[(x_1, \phi(n)) = (y_1, \phi(n)) = 1. \]
The similarity between the algorithms AM and AL is clear. It follows that any Mental Poker instance \((m^y \bmod n), m^x \bmod n, m^y \bmod n)\) is actually a Diffie-Hellman instance \((a, a^x \bmod n, a^y \bmod n)\) where both \(a^x, a^y \bmod n\) belong to \(C(a)\) and not just to \(B(a)\). By this observation it follows that AM is well-defined (Lemma 5). Also analogues of Definition 6 can be made omitting the parentheses there. In particular, a \((\frac{1}{F_1}, \frac{1}{F_2})\)-admissible base element for the algorithm AM is actually a \((\frac{1}{F_1}, \frac{1}{F_2})\)-C admissible base element when AM is considered as a composite Diffie-Hellman cracking algorithm.

Despite the close resemblance between the algorithms AM and AL note that Mental Poker can only be played when both partners know the secret decomposition of \(n\). On the other hand, in the Diffie-Hellman composite system there is clearly no need to know the factorization of \(n\) in order to generate the common keys \(X_{ij} = a^{x_i y_j} \bmod n\).

5. CRACKING COMPOSITE DIFFIE-HELLMAN SYSTEMS IS AT LEAST AS HARD AS FACTORING

Here we prove that cracking the composite Diffie-Hellman system is at least as hard as the factorization of a composite number \(n\). A similar result holds for cracking Mental Poker Playing. In the following, we let \(\tau(n)\) stand for the average number of steps needed to find \(\gcd(u,v)\) for \(u,v < n\) (see [8]).

Theorem 7: Let \(n=pq\) be a composite number where \(p, q\) are primes satisfying (4), (5). Also let the algorithm AL given in (14)\(^*\) crack the composite Diffie-Hellman system in \(F(n)\) steps for all proper inputs. Given that \(\frac{1}{F_0}\) of all base elements \(a \in \mathbb{G}(n)\) are \((\frac{1}{F_1}, \frac{1}{F_2})\)-admissible AL can be used for factor \(n\) in at most \(2^{k+2-1} F_0 f_1 f_2 G(n)\) steps on the average where \(G(n) = F(n) + 8\log_2 n + \tau(n) + 2\).
Note that \( 2^{k+2-1} \leq \frac{e^5}{2} \) is rather small when \( n \) is a hard to factor number, see Corollary (4).

Proof: Choose an element \( c \in \mathbb{Z}^*_n \) and let \( a \equiv c^2 \pmod{n} \). Considering the characterization of the set \( Q(n) \) given in Theorem 3 together with Corollary 4 we find that there is a probability of \( \left(\frac{1}{2}\right)^{k+2-2} \) that \( a \equiv c^2 \in Q(n) \). By (ii), Theorem 3, the mapping \( x \rightarrow x^2 \pmod{n} \) is one-to-one and onto \( Q(n) \) with the inverse \( x \rightarrow x^{t_1} \pmod{n} \) for \( t_1 \) given in (13). Thus, there is a probability \( \frac{1}{f_o} \) that \( a^2 \pmod{n} \) is a \((\frac{1}{f_1}, \frac{1}{f_2})\)-admissible base element for the algorithm \( AL \) provided that \( a \in Q(n) \).

Picking at random exponents \( 1 \leq r_1, r_2 \leq n \) it follows that with a probability \( \geq \frac{1}{f_1 f_2} \) the triple \( (a, a^{r_1} \pmod{n}, a^{r_2} \pmod{n}) \) is proper for \( AL \) (here \( a \equiv (a) \dagger r \) where \( (t_1, \phi(n)) = 1 \) holds for each \( r \)).

In such a case

\[
AL(a \pmod{n}, a^{r_1} \pmod{n}, a^{r_2} \pmod{n}) = J
\]

where by (16) \( J \equiv a^{t_1 r_1 r_2} \pmod{n} \) holds. Since \( a^{t_1} \equiv a \pmod{n} \) we find that \( J^2 \equiv a^{2t_1 r_1 r_2} \pmod{n} \) implying that \( J \) is a quadratic root of \( a^{r_1 r_2} \pmod{n} \). Because \( a \equiv c^2 \pmod{n} \) it follows that \( c^{r_1 r_2} \pmod{n} \) is also a quadratic root of \( a^{r_1 r_2} \pmod{n} \). With probability \( \frac{1}{2} \)

\[
J \neq t_1 r_2 \pmod{n} \) holds, in which case \( \gcd(J-c^{r_1 r_2} \pmod{n}), n) \) is a proper factor of \( n \). Considering one modular multiplication as a single step it follows that for each choice of \( c, r_1, r_2 \) at most \( E(n) + 8 \eta n + 2 + \gamma(n) \) computational steps have to be performed on the average. The probability of success for such a choice was shown to be \( \geq \frac{1}{2} \left(\frac{1}{2^{k+2-2} f_1 f_2} \right) \) which ends the proof.
By repeating the proof of the last theorem and choosing the numbers $r_1, r_2$ to be relatively prime to $\phi(n)$ (this has a probability of $\left(\frac{1}{\phi(n)}\right)^2$), we get

Theorem 8: Let $n = pq$ be a composite number where $p, q$ are primes satisfying (4), (5). In addition, let the algorithm $AM$ given in (19) crack Mental Poker Playing in $P(n)$ steps for all its proper inputs. If $\frac{1}{r_0}$ of all base elements $a \in \mathbb{Q}(n)$ are $(\frac{1}{r_1}, \frac{1}{r_2})$-admissible for $AM$, then $AM$ can be used to factor $n$ in at most

$$2^{k+2} - \frac{1}{r_0} \cdot \frac{1}{r_1} \cdot \frac{1}{r_2} \left(\frac{n}{\phi(n)}\right)^2 \cdot G(n)$$

steps, where $G(n) = P(n) + 2\log_2(n) + 2$.


6. CRACKING COMPOSITE DIFFIE-HELLMAN SYSTEMS IS AT LEAST AS HARD AS CRACKING RSA

In the last section we have demonstrated the cryptographic strength of the composite Diffie-Hellman system as well as that of Mental Poker Playing. This was achieved by using algorithm $AL$ (resp. $AM$) for which $\frac{1}{r_0}$ of all $a \in \mathbb{Q}(n)$ were assumed to be admissible.

As noted in Corollary 4, $\mathbb{Q}(n)$ is quite large, $|\mathbb{Q}(n)| = \frac{(n-1)(q-1)}{2^{k+2}} > p'q'$.

In this section we prove that even when relaxing the assumptions on the distribution of admissible base elements, the Diffie-Hellman cracking algorithm $AL$ is still powerful enough so as to crack the RSA-encryption scheme $(e, n)$, see [4]. A similar result holds for $AM$, the algorithm cracking Mental Poker, due to the analogy between both algorithms.

Recall that when given $n, l \leq e \leq n$, where $\gcd(e, \phi(n)) = 1$, the message $m, 1 \leq m \leq n$, may be a RSA-encrypted by $c \equiv m^e \pmod{n}$. $c$ can then be decrypted provided that a multiplicative inverse $e^*$ of $e$ modulo $\phi(n)$
is known since \( c^e \equiv (m^s)^e \equiv m \pmod{n} \). The parameters \( e, n \) of the RSA-scheme are publicly known whereas \( c^e \) is kept secret by the receiver of the message, see [4]. We now prove

Theorem 9: Let \((e, n)\) be a given RSA public key encryption scheme.

Also let the algorithm AL given in (14)\(^*\) crack the composite Diffie-Hellman system in \( F(n) \) steps for all its proper inputs. Given that AL is \((\frac{1}{f_0}, \frac{1}{f_1}, \frac{1}{f_2})\)-C admissible, it can be used to crack any RSA-encrypted message \( c \equiv m^e \pmod{n} \) in at most \( \frac{e}{\phi(n)} \cdot \left( \frac{\phi(n) - e}{\phi(e)} \right)^2 G(n) \) steps on the average where \( G(n) = F(n) + \frac{161g_2 n + r(n^2 + 3)}{} \).

Note that by (4) \( \frac{\phi(n)}{\phi(e)} \approx \frac{e}{\phi(e)} \) is rather small.

Proof: Choose at random an element \( x \in \mathbb{Z}_n^* \) and let \( b \equiv (x^e c)^e \pmod{n} \).

Since \( f: x \mapsto (x^e c)^e \pmod{n} \) maps \( \mathbb{Z}_n^* \) onto itself it follows that \( b \) is \((\frac{1}{f_0}, \frac{1}{f_1}, \frac{1}{f_2})\)-C admissible for AL with probability \( \geq \frac{1}{f_0} \) (we may assume that \( c \equiv \mathbb{Z}_n^* \) otherwise \((C, n)\) yields the factorization of \( n \).

For any proper input triple \( \Gamma = (b, b^u \pmod{n}, b^v \pmod{n}) \) we may write \( b \equiv b^u \pmod{n} \) and \( b \equiv b^v \pmod{n} \) due to the invertibility of \( e \) modulo \( \phi(n) \) (take \( e.g., r_o = eu, s_o = ev \)). By letting \( a \equiv b^{-e} \equiv x^{-e} c \pmod{n} \) we get \( \Gamma = (a^e \pmod{n}, a^r \pmod{n}, a^s \pmod{n}) \).

By Lemma 2 it follows that \( \frac{\phi(e)}{e} \) of all representing exponents \( r_i \) of all representing exponents \( s_i \) where \( a \equiv a_o = b^e r_o = b^u \pmod{n} \) satisfy \( (r_i, e) = 1 \). Similarly, \( \frac{\phi(e)}{e} \) of all representing exponents \( s_i \) where \( a \equiv a_o = b^e s_o = b^v \pmod{n} \) satisfy \( (s_i, e) = 1 \). Picking at random exponents \( 1 \leq r, s \leq n \) so that \( (r, \phi(n)) = (s, \phi(n)) = (r, e) = (s, e) = 1 \) (this can be done with probability \( \left( \frac{\phi(n)}{n} \right)^2 \)) since \((e, \phi(n)) = 1 \) there is a probability \( \geq \frac{1}{f_0} \) that the input triple \((a^e \pmod{n}, a^r \pmod{n}, a^s \pmod{n})\)
is proper for \( AL \). By (17) it follows that

\[
(20) \quad AL(a^e \mod n), a^x \mod n, a^s \mod n) = \mathbb{Z} \equiv a^{e+rs} \mod n.
\]

Since \( c \equiv m^e \mod n \) it follows that

\[
J \equiv a^{e+rs} \equiv (x^e)^r \cdot s^r \equiv (x^e)^r \mod n.
\]

We now find \( D = J \cdot r \cdot (x^e)^r \mod n \) where obviously \( D = m^{rs} \mod n \).

Since both \( x, s \) are relatively prime to \( e \), the Euclidean gcd algorithm can be used to find integers \( f_1, f_2 \) satisfying \( f_1e + f_2rs = 1 \).

By computing

\[
\frac{f_1}{c} D = (m^e)^{f_1} (m^{rs})^{f_2} = m^{f_1e + f_2rs} = m \mod n
\]

the secret message \( m \) is found. Since the probability of success is

\[
\geq \frac{1}{e \cdot 1 \cdot 2} \left( \frac{\phi(n) \cdot \phi(e)}{\phi(n) \cdot e} \right)^2
\]

and approximately \( G(n) = F(n) + 16 \log_2 n + \tau(n^2) + 3 \) computational steps have to be made for each choice of \( r, s, x \) the proof is complete (a modular division or multiplication is considered a basic step). \( \square \)

We omit the formulation of a precise analogue of Theorem 9 for an algorithm \( AM \) cracking Mental Poker Playing.

7. GENERALIZED DIFFIE-HELLMAN KEY-GENERATING SYSTEMS

Generalized composite Diffie-Hellman key generating systems were described in §1, see (3), (3) * there. One can easily show as in Lemma 5 that any algorithm \( AL_{s,n} \) which cracks such a system is well-defined, i.e., its value \( K_{12...s} \) where

\[
(21) \quad AL_{s,n}(n, s, a, x_1, i_2, \ldots, i_r \equiv a_1^{x_1} a_2^{x_2} \cdots a_r^{x_r}, \text{ for all } 1 \leq i_1 < i_2 < \ldots < i_r \leq s,
\]

and all \( 1 \leq r < s \) \( = a_1^{x_1} a_2^{x_2} \cdots a_r^{x_r} \mod n \) \( \equiv K_{12...s} \)
is not dependent on the particular exponents chosen to represent the $a^{s-2}$ "intermediate" keys $x_{i_1}^{i_2}...i_r$, $1 \leq r < s$. Concerning these systems the following holds

**Theorem 10:** Let $AL_{s,n}$ given in (21) denote an algorithm which cracks a generalized composite Diffie-Hellman key-generating system in $F(n,s)$ steps for at least $\frac{1}{t_0}$ of all base elements $a \in Q(n)$. Then $AL_{s,n}$ can be used to factor $n$ in at most $2^{k+\ell-2}t_0G(s,n)$ steps on the average where $G(s,n) = F(s,n) + \tau(n) + (4\log_2 n + s)2^{s-1}$.

**Proof:** Choose $c \in Z_n^*$ and assume that $\hat{a} = c^2(\mod \ n) \in Q(n)$.

By Theorem 3 this happens with probability $\frac{1}{2^{k+\ell-2}}$. Assume also that $a = \hat{a}2^{s-1} \ (\mod \ n)$ is an admissible base element for $AL_{s,n}$ (this happens with probability at least $\frac{1}{t_0}$) and choose arbitrary exponents $1 \leq x_1 \leq x_2 \leq \ldots \leq x_k \leq n$. Now use $AL_{s,n}$ to find $J$ given by

$$
AL_{s,n}(n,s,a) = \hat{a}^{2^{s-1}x_1}, \ldots, \hat{a}^{2^{s-1}x_{k}}, \ldots
$$

(22) $AL_{s,n}(n,s,a) = \hat{a}^{2^{s-1}x_1}, \ldots, \hat{a}^{2^{s-1}x_k}, \ldots$

$$
= \hat{a}^{2^{s-1}x_1}, \ldots, \hat{a}^{2^{s-1}x_s}, \ldots
$$

Since $\hat{a} \in Q(n)$, $\hat{a}^{2t} = \hat{a}(\mod \ n)$ holds for some $t$, hence

$$
\hat{a}^{2^{s-1}x_1}, \ldots, \hat{a}^{2^{s-1}x_s}, \ldots = \hat{a}^{2^{s-1}x_1}, \ldots, \hat{a}^{2^{s-1}x_s}, \ldots
$$

for any $1 \leq i_1 \leq i_2 \leq \ldots \leq i_r \leq s$, $1 \leq r < s$. By (21) we find replacing $x_i$ by the corresponding $tx_i$, $1 \leq i \leq s$, that

$$
J \equiv \hat{a}^{2^{s-1}tx_i}, \ldots, \hat{a}^{2^{s-1}tx_s}, \ldots \equiv \hat{a}^{2^{s-1}tx_i}, \ldots, \hat{a}^{2^{s-1}tx_s}, \ldots (\mod \ n)
$$

and so

$$
J^2 \equiv (\hat{a}^{2^{s-1}tx_i}, \ldots, \hat{a}^{2^{s-1}tx_s}, \ldots) \equiv \hat{a}^{2^{s-1}tx_i}, \ldots, \hat{a}^{2^{s-1}tx_s}, \ldots (\mod \ n)
$$

Since $\hat{a} = c^2(\mod \ n)$ it follows
that both $c$ and $J$ are quadratic roots of $a^x_1 x_2 \cdots x_s$ modulo $n$.

Thus, with probability $\frac{1}{2}$ a proper factor of $n$ is obtained by

$$\gcd(J-C^1 r^2 \cdots r^s \pmod{n}, n).$$

Taking account of the various computations performed, the proof is completed.

\[\square\]

**APPENDIX**

**Proof of Lemma 2**

The proof follows easily using (11), Lemma 1 and noting that

$$M = \frac{(p-1)(q-1)}{\xi_1, \xi_2}$$

satisfies $(M, e) = 1$. Consequently, the equation

$$x_1 - x_0 \equiv \theta x (\pmod{e})$$

with unknown $\theta$ is uniquely solvable modulo $e$ for any $x_1$ ([7], p.113). Since $\frac{\phi(e)}{e}$ of the elements $x_i$ satisfy $(x_i, e) = 1$ the lemma follows.

\[\square\]

**Proof of Theorem 3**

(i) $\Rightarrow$ (v): Using the representation of $a$ by the cyclic generators $g, h$ given in (9), (i) yields

$$2t\alpha = a + \theta_1 (p-1), \quad 2t\beta = \beta_2 (q-1)$$

for some $\theta_1, \theta_2$. By (5), (6), we get

$$\alpha(2t-1) = \theta_1 2^k \cdot p, \quad \beta(2t-1) = \theta_2 2^k \cdot q.$$  

Since $p, q$ and $2t-1$ are odd $2^k \mid \alpha, 2^k \mid \beta$ follows implying (v).

Conversely, if $\alpha = 2^k \theta_1, \beta = 2^k \theta_2$ in (9) then (23) holds when taking

$$2t-1 = \frac{\theta_{\alpha, \beta}}{p, q}$$

for any odd integer $\theta$ and (i) follows easily.
(v) \( \Rightarrow \) (ii): Assuming (v) it is easy to show that \( t_1 \) given in (13) is relatively prime both to \( p-1 \) and \( q-1 \) hence to \( \phi(n) \). Clearly,
\[
2t_1 = 2a_1^2 \equiv g^{2k_1} \equiv g^{(1+\theta p_q)} \equiv g^{2k_1} \equiv a \pmod{p}.
\]
Similarly
\[
a^{2k_1} \equiv a \pmod{q} \text{ which by the Chinese Remainder Theorem implies (ii).}
\]
Since (ii) \( \Rightarrow \) (i) is clear we have (ii) \( \Rightarrow \) (v) by the first part.
(iv) \( \Rightarrow \) (iii) \( \Rightarrow \) (v) \( \Rightarrow \) (iv); (iv) \( \Rightarrow \) (iii) Since \( \phi(n) \) is an even number. Assuming (iii) and using (8) we get \( 2^a \equiv q^k \pmod{p} \),
\[
h^2 = h^k \pmod{q}.
\]
Thus
\[
a(2-s) = 6_1(p-1) = 6_1 2^k p, \quad \beta(2-s) = 6_2(q-1) = 6_2 2^k q.
\]
Here \( 2-s \) is an odd number so \( 2^k | \alpha \), \( 2^k | \beta \) must hold implying (v).
To complete the proof assume conversely that (v) holds. Now
\[
s_1 = 2 + \frac{p \cdot q}{(p, q)} \text{ is obviously relatively prime to } \phi(n). \quad \text{Since}
\]
\[
\alpha s_1 = 2^k a_1 (2 + \frac{p \cdot q}{(p, q)}) = 2^{k+1} a_1 + 2^k p = 2^a + \theta(p-1) \quad \text{we find that}
\]
\[
a^{s_1} \equiv g^{s_1} \equiv g^{2a+\theta(p-1)} \equiv g^{2a} \equiv a^2 \pmod{p}.
\]
Similarly \( a^{s_1} \equiv a^2 \pmod{q} \) holds whence \( a^{s_1} \equiv a^2 \pmod{n} \). Thus (iv) follows and the proof is complete.

\[\square\]

**ACKNOWLEDGEMENT**

The author wishes to thank Professor Adi Shamir for his most helpful suggestions.
REFERENCES


