Generalised Discrete Log Problem

Saturday, 7 December 2019 11:33 AM

DLP: Given $b, \beta \in \mathbb{Z}_p^*$, primitive element α
find x s.t. $\alpha^x \equiv \beta \bmod p$

DIFFIE-HELLMAN PROBLEM (DHP)
Recall: D-H key exchange

ALICE $\xleftarrow{\alpha, \beta}$ BOB

$a = k_{priv,A} \in \{2, \dots, p-2\}$ $\quad b = k_{priv,B} \in \{2, \dots, p-2\}$

$A = k_{pub,A} = \alpha^a \bmod p \xrightarrow{A}$ $\quad \xleftarrow{B} B = k_{pub,B} = \alpha^b \bmod p$

over insecure connection

$K_{AB} = B^a \bmod p$ $\quad K_{AB} = A^b \bmod p$

Security:
assume OSCAR is a passive attacker ie
he can only listen (!!)
∴ he knows α, p, A, B
what he wants K_{AB} ?? (ie DHP)
Approach (1):
(1) compute $a = \log_\alpha A \bmod p$
(2) then he can do B^a to get K_{AB}
UNFORTUNATELY for OSCAR
(1) is COMPUTATIONALLY A VERY HARD PROBLEM if p is large enough

∴ If the only way of solving the DHP requires the DLP, one would say that "the DHP is equivalent to the DLP"
However this is not proven (YET).

In the case of RSA the situation is SIMILAR: Factorisation is not necessarily the only way to break RSA.

GENERALISED DLP or GDLP:
one powerful feature of the DLP not restricted to $\mathbb{Z}_p^*$ but other cyclic groups can also be used for building DL crypto-systems.

$G_1 = \{\alpha, \alpha^1, \alpha^2, \dots, \alpha^{|G|-1}\}$
$\alpha \rightarrow$ primitive element

GENERALISED DLP:
Given DLP, Given cyclic $(G, \circ)$ and $|G| = n$. Let α be primitive element and $\beta \in G$.
Find x s.t. $\beta = \alpha \circ \alpha \circ \dots \circ \alpha$
x times

ATTACKS

Goal: solve $\log_\alpha \beta = x$
$\alpha, \beta \in G$, $n = |G|$, $\alpha^x = \beta$

(1) BRUTE FORCE.
$\alpha^1 \stackrel{?}{=} \beta$
$\alpha^2 \stackrel{?}{=} \beta$
⋮
requires $O(n)$ steps
If this is the only attack, then
$n \gtrsim 2^{80}$

(2) SQUARE-ROOT-ATTACKS
(baby step giant step algorithm)
and
(Pollards rho method)
compute x in $O(\sqrt{n})$ steps.
if $n \approx 2^{80}$ $\sqrt{n} = \sqrt{2^{80}} = 2^{40}$
for 80 bit string $\Rightarrow$ $n \approx 2^{160}$

Important square root attack work in any group. For elliptic curves, rho are the best known ATTACKS

[HAC, Alg 3.56, Alg 3.60]

(3) Index-calculus attacks:
for certain groups, G_1 the more powerful exist, in particular, the attacks works in $\mathbb{Z}_p^*$ and $\mathbb{F}(2^n)$.
In practise $p, 2^n \gtrsim 2^{1024}$
∴ often $p \rightarrow 2^{1024} \dots 2^{2048}$ bits

[HAC, Alg 3.68]
↳ HANDBOOK of APPLIED CRYPTOGRAPHY

primitive element and $\beta \in G_1$.
Find x s.t. $\beta = \underbrace{\alpha \circ \alpha \cdots \circ \alpha}_{x \text{ times}}$.

$$= \begin{cases} \alpha^x, & \text{if } \circ = \text{multiply} \\ x \cdot \alpha, & \text{if } \circ = \text{add} \end{cases}$$

Q: which other cyclic groups make good DL problems?

PRACTICAL
(1) $\mathbb{Z}_p^*$: multiplicative group of a prime field.
(2) $GF(2^m)^k$: " " " "
extension field.

(3) Elliptic curve: the group consists of points on a curve.
(4) Generalisations of (3)
eg: hyperelliptic curves.