

ROUND 2

$T = (05884C89 * (2 * 05884C89 + 1))$ SHIFT LEFT TO $\text{LOG}_2 32$

$= (05884C89 * (B109913))$ SHIFT LEFT TO $\text{LOG}_2 32$

$= 3D371D8A6B8F2B$ SHIFT LEFT TO $\text{LOG}_2 32$

$= 8A6B8F2B$ SHIFT LEFT TO $\text{LOG}_2 32$

$= 8A6B8F2B$ SHIFT LEFT TO 5

$= 4D71E571$

$U = (C93C6CB1 * (2 * C93C6CB1 + 1))$ SHIFT LEFT TO $\text{LOG}_2 32$

$= (C93C6CB1 * (9278D963))$ SHIFT LEFT TO $\text{LOG}_2 32$

$= 73237531EF781173$ SHIFT LEFT TO $\text{LOG}_2 32$

$= EF781173$ SHIFT LEFT TO $\text{LOG}_2 32$

$= EF781173$ SHIFT LEFT TO 5

$= EF022E7D$

$A = ((327EEE86 \text{ XOR } 4D71E571) \lll EF022E7D) + 304F5797$

$= (7F0F0BF7 \lll EF022E7D) + 44E8988B$

$= EFE1E17E + 44E8988B$

$= 34CA7A09$

$C = ((A62264A3 \text{ XOR } EF022E7D) \lll 4D71E571) + C78149C2$

$= (49204ADE \lll 4D71E571) + C78149C2$

$= 95BC9240 + C78149C2$

$= 5D3DDC02$

A = 05884C89
B = 5D3DDC02
C = C93C6CB1
D = 34CA7A09

ANSWER ROUND 3 AND 4

A = 05884C89
B = 5D3DDC02
C = C93C6CB1
D = 34CA7A09

S6=b517132e
S7=93f42a72
S8=4747770F
S9=c045fe0e

ROUND 3

$T = (5D3DDC02 * (2 * 5D3DDC02 + 1))$ SHIFT LEFT TO $\text{LOG}_2 32$
 $= (5D3DDC02 * (BA7BB805))$ SHIFT LEFT TO $\text{LOG}_2 32$
 $= 43EC0198714CBC0A$ SHIFT LEFT TO $\text{LOG}_2 32$
 $= 714CBC0A$ SHIFT LEFT TO $\text{LOG}_2 32$
 $= 714CBC0A$ SHIFT LEFT TO 5
= 2997814E

$U = (34CA7A09 * (2 * 34CA7A09 + 1))$ SHIFT LEFT TO $\text{LOG}_2 32$
= $(34CA7A09 * (6994F413))$ SHIFT LEFT TO $\text{LOG}_2 32$
= 15C5C371258BA2AB SHIFT LEFT TO $\text{LOG}_2 32$
= 258BA2AB SHIFT LEFT TO $\text{LOG}_2 32$
= 258BA2AB SHIFT LEFT TO 5
= **B1745564**

$A = ((05884C89 \text{ XOR } 2997814E) \lll B1745564) + b517132e$
= $(2C1FCDC7 \lll B1745564) + b517132e$
= C1FCDC72+ b517132e
= **7713EFA0**

$C = ((C93C6CB1 \text{ XOR } B1745564) \lll 2997814E) + 93f42a72$
= $(784839d5 \lll 2997814E) + 93f42a72$
= 0E755E12+ 93f42a72
= **A2698884**

A=5D3DDC02

B= A2698884

C=34CA7A09

D=7713EFA0

ROUND 4

$T = (A2698884 * (2 * A2698884 + 1))$ SHIFT LEFT TO $\text{LOG}_2 32$
= $(A2698884 * (44D31109))$ SHIFT LEFT TO $\text{LOG}_2 32$
= $2BA9F00D4C9290A4$ SHIFT LEFT TO $\text{LOG}_2 32$
= $4C9290A4$ SHIFT LEFT TO $\text{LOG}_2 32$
= $4C9290A4$ SHIFT LEFT TO 5
= **92521489**

$U = (7713EFA0 * (2 * 7713EFA0 + 1))$ SHIFT LEFT TO $\text{LOG}_2 32$
= $(7713EFA0 * (EE27DF41))$ SHIFT LEFT TO $\text{LOG}_2 32$
= $6EC714A8DB2C37A0$ SHIFT LEFT TO $\text{LOG}_2 32$
= $DB2C37A0$ SHIFT LEFT TO $\text{LOG}_2 32$
= $DB2C37A0$ SHIFT LEFT TO 5
= **6586F41B**

$A = ((5D3DDC02 \text{ XOR } 92521489) \lll 6586F41B) + 4747770F$
= $(cf6fc88b \lll 6586F41B) + 4747770F$
= $5E7B7E44 + 4747770F$
= **A5C2F553**

$C = ((34CA7A09 \text{ XOR } 6586F41B) \lll 92521489) + c045fe0e$
= $(514c8e12 \lll 92521489) + c045fe0e$
= $991C24A2 + c045fe0e$
= **596222B0**