Analysis

Given:

$$(a_1, password * g^{a_1}) = (324, 1122681535026353181496333631 5)$$

$$(a_1, password * g^{a_1}) = (324, 11226815350263531814963336315)$$

$$(a_1, password * g^{a_1}) = (324, 11226815350263531814963336315)$$

we want to find password given elements are multiplicative group Z_p^* where

p=19807040628566084398385987581 is prime

$$password * g^{a_1} \equiv A_1(mod\ \ p) ------(i)$$

$$password * g^{a_2} \equiv A_2(mod\ \ p) ------(ii)$$

$$password * g^{a_3} \equiv A_3(mod\ \ p) ------(iii)$$

Multiplying and dividing left hand side of equation 2 and 3 from g^{a_1}

$$(password * g^{a_1}) * g^{(a_2-a_1)} \equiv A_2(mod\ \ p)$$

$$(password * g^{a_1}) * g^{(a_3-a_1)} \equiv A_3(mod\ \ p)$$

Using Property: $(a * b)(mod\ \ m) \equiv a(mod\ \ m) * b(mod\ \ m)$

$$((password * g^{a_1}))(mod\ \ p) * g^{(a_2-a_1)}(mod\ \ p) \equiv A_2(mod\ \ p)$$

$$(password * g^{a_1})(mod\ \ p) * g^{(a_3-a_1)}(mod\ \ p) \equiv A_3(mod\ \ p)$$

Using equation (i) we can substitute $((password * g^{a_1})(mod\ \ p))$

get equation (iv) (v)

$$A_1 g^{(a_3-a_1)} \equiv A_3(mod\ \ p) ------(iv)$$

$$A_1 g^{(a_2-a_1)} \equiv A_2(mod\ \ p) ------(v)$$

$$a_3 - a_1 = 9513 - 324 = 9189$$

$$a_2 - a_1 = 2345 - 324 = 2021$$

we found X and Y. And now apply Extended Euclidean Algorithm

X	Y	q	r	l_1	l_2	l_3	m_1	m_2	m_3
9189	2021	4	1105	1	0	1	0	1	-4
2021	1105	1	916	0	1	-1	1	-4	5
1105	916	1	189	1	-1	2	-4	5	-9
916	189	4	160	-1	2	-9	5	-9	41
189	160	1	29	2	-9	11	-64	41	-50
160	29	5	15	-9	11	-64	41	-50	291
29	15	1	14	11	-64	75	-139	-291	-341
15	14	1	1	-64	75	-139	-291	-341	632
14	1	14	0	75	-139	2021	-341	632	-9189

So, we found the following:

$$gcd(9189, 2021) = 1 - - - - - - - - (vi)$$

$$l = -139 \ \ and \ \ m = 632$$

Using Extended Euclid Algorithm

$$X_l + Y_m = gcd(X, Y)$$

From Equation (vi) we Know $gcd(X, Y) = 1$

$$X_l + Y_m = 1 - - - - - (vii)$$

$$(A_1^l \ g^{Xl}) \equiv A_3^l \ (mod \ \ p) - - - - - (viii)$$

$$A_1^m \ g^{Ym} \equiv A_3^m \ (mod \ \ p) - - - - - - - - (xi)$$

multiply equation (viii) and (xi)

$$A_1^{(l+m)} * g^{(Xl+Ym)} \equiv (A_3^l * A_2^m)(mod \ \ p)$$

Using Equation (vii)

$$A_1^{(l+m)} * g \equiv (A_3^l * A_2^m)(mod \ \ p)$$

$$(A_3^l * A_2^m) mod \ \ p \equiv ((A_3^l (mod \ \ p)) * (A_2^m mod \ \ p)) mod \ \ p$$

l=139 so find $(A_3^l (mod \ \ p))$ for l=139 then find the multiplicative inverse of that number. i.e $A_3^l * A_3^{-l} (mod \ \ p) = 1$

Now if we take RHS as $num = (A_3^l * A_2^m)(mod \ \ p)$

$$A_3^{139} mod \ \ p = 1438737264732336067040734445$$

$$A_2^{(632)} mod \ \ p = 9086425608952457377582771788$$

Using above values we get value of num:

$$num = 11099199913639351335199364706$$

now equation become

$$A_1^{(l+m)} * g \equiv num ------(x)$$

we know that

$$(a * b) mod\ \ p \equiv num$$

$$b \equiv (a^{-1} * num) mod\ \ p$$

now equation (x) becomes

$$g \equiv (A_1^{-(l+m)} * num) mod\ \ p$$

again we have to find modular inverse of $A_1^{(l+m)}$
value of $A_1^{(l+m)} = 26090206188876238800099546994$ lets take

$$a = A_1^{-(l+m)}$$

Value of a = 11763215952453956375186720348
now our equation became

$$g \equiv (a * num) mod\ \ p ------(xi)$$

now find g from equation (xi) g = 192847283928500239481729 then for finding password lets take equation (ii) we can take any equation (i),(ii),(iii)

$$password * g^{a_2} \equiv A_2 mod\ \ p ------(ii)$$

We know g, a_2, A_2 and p

$$password \equiv (A_2 * g^{-a_2}) mod\ \ p ------(xii)$$

find multiplicative inverse of g^{a_2} and put equation (xii)

$$g^{-a_2} = 6507145214719002336566928446$$

we get password from equation (xii)
password = 3608528850368400786036725