Stack	Project	Comments
<cafe signature=""> 15, 105</cafe>	<cafe signature="??,???"> <cafe key="??" public=""> DUP</cafe></cafe>	
	HASH160 < Cafe Public Key Hash=?> EQUALVERIFY	<sig>   <sig> <pubk> DUP HASH160</pubk></sig></sig>
	CHECKSIG	<pubkhash> EQUALVERIFY CHECKSIG</pubkhash>
	^	۸
	I	I
	Value <sig> is pushed to the top of the stack</sig>	Value <sig> is pushed to the top</sig>
		of the stack
	Cafe Signature = Bob's signature	
	O Step 1: Create a hash of the	
	Alice's transaction (43) concatenated with	
	Gopesh's <u>public key</u> .	
	0	
	Gopesh's public key = $k*G = 7*5 = 35$	
	==> HASH = 4335 % 3 = 0	
	0	
	O Step 2: Encrypt the hash with	
	Bob's private key (3)	
	0	
	0 ==>	
	0	
	0	
	C1 = PR(Bob)*G = 3*5=15	
	0	
	C2 = Hash + PR(Bob) * PU(Gopesh) =	
	0+3*35=105	
Cafe Public Key> 15	<cafe signature="??,???"> <cafe key="??" public=""> DUP</cafe></cafe>	<pubk></pubk>
	HASH160 <cafe hash="?" key="" public=""> EQUALVERIFY</cafe>	<sig>   <sig> <pubk> DUP HASH160</pubk></sig></sig>
<cafe signature=""> 15, 105</cafe>	CHECKSIG	Sig>   Sig> Fubk> DUF HASH100 PubKHash> EQUALVERIFY CHECKSIG
	A	A VERTICAL PERIOD CHECKSTO
	Value Cafe Dublic Vary is muched to the	Value (DukVa is much ad to
	Value <cafe key="" public=""> is pushed to the</cafe>	Value <pubk> is pushed to</pubk>
	stack, on top of <sig></sig>	the stack, on top of <sig></sig>
	Cafe Public Key = Bob's Public Key = 15	-

<cafe key="" public=""> 15</cafe>	<cafe signature="??,???"> <cafe key="??" public=""> DUP</cafe></cafe>	<pubk></pubk>
<cafe key="" public=""> 15</cafe>	HASH160 <cafe hash="?" key="" public=""> EQUALVERIFY</cafe>	<pubk></pubk>
<cafe signature=""> 15, 105</cafe>	CHECKSIG	<sig>   <sig> <pubk> DUP HASH160</pubk></sig></sig>
	۸	<pubkhash> EQUALVERIFY CHECKSIG</pubkhash>
	ı	^
	DUP operator duplicates the top item in the	I
	stack,	DUP operator duplicates the
	the resulting value is pushed to the top of the	top item in the stack,
	stack	the resulting value is pushed
		to the top of the stack
<cafe hash="" key="" public=""> 0</cafe>	<pre><cafe signature="??,???"> <cafe key="??" public=""> DUP</cafe></cafe></pre>	<pubkhash></pubkhash>
<cafe key="" public=""> 15</cafe>	HASH160 < Cafe Public Key Hash=?> EQUALVERIFY	<pubk></pubk>
<cafe signature="">15, 105</cafe>	CHECKSIG	<sig>   <sig> <pubk> DUP HASH160</pubk></sig></sig>
	^	<pubkhash> EQUALVERIFY CHECKSIG</pubkhash>
		^
	HASH160 operator hashes the top item in	I
	the stack with	HASH160 operator hashes
	RIPEMD160(SHA256(PubK)), the	the top item in the stack with
	resulting value (Cafe Public Key Hash)	
	is pushed to the top of the stack	RIPEMD160(SHA256(PubK)), the resulting
		value (PubKHash)
	Cafe Public Key Hash = Bob Public Key Hash = 15 % 3 = 0	is pushed to the top of the stack
<cafe hash="" key="" public=""> 0</cafe>	<cafe signature="??,???"> <cafe key="??" public=""> DUP</cafe></cafe>	<pubkhash></pubkhash>
<cafe hash="" key="" public=""> 0</cafe>	HASH160 < Cafe Public Key Hash=?> EQUALVERIFY	<pubkhash></pubkhash>
<cafe key="" public=""> 15</cafe>	CHECKSIG	<pubk></pubk>
<cafe signature=""> 15, 105</cafe>		<sig>   <sig> <pubk> DUP HASH160</pubk></sig></sig>
	^	<pubkhash> EQUALVERIFY CHECKSIG</pubkhash>
		٨
	The value <cafe hash="" key="" public=""> from</cafe>	
	the script is pushed on the top of	
	the value <cafe hash="" key="" public=""></cafe>	The value PubKHash from
	calculated previously from	the script is pushed on the top of
	the HASH160 of the <cafe key="" public="">.</cafe>	the value PubKHash
		calculated previously from
		the HASH160 of the
		PubK.

<cafe key="" public=""> 15</cafe>	<cafe signature="??,???"> <cafe key="??" public=""> DUP</cafe></cafe>	<pubk></pubk>
<cafe key="" public=""> 15 <cafe signature=""> 15, 105</cafe></cafe>		
	HASH160 <cafe hash="?" key="" public=""> EQUALVERIFY</cafe>	<pre><sig>   <sig> <pubk> DUP HASH160</pubk></sig></sig></pre>
	CHECKSIG	<pubkhash> EQUALVERIFY CHECKSIG</pubkhash>
	^	
	I	
	The EQAULVERIFY	The EQAULVERIFY
	operator compares the PubKHash encumbering	operator compares the PubKHash
	the transaction with the	encumbering
	PubKHash calculated from	the transaction with the
	the user's PubK. If they	PubKHash calculated from
	match, both are removed and	the user's PubK. If they
	execution contines	match, both are removed and
		execution contines
TRUE	<cafe signature="??,???"> <cafe key="??" public=""> DUP</cafe></cafe>	TRUE   <sig> <pubk> DUP HASH160</pubk></sig>
	HASH160 < Cafe Public Key Hash=?> EQUALVERIFY	<pubkhash> EQUALVERIFY CHECKSIG</pubkhash>
	CHECKSIG	
		^
	^	
		The CHECKSIG operator
	The CHECKSIG operator checks	checks that the signature <sig></sig>
	that the signature <cafe signature=""></cafe>	matches the public key
	matches the public key &tPubK>	
	and pushes TRUE	to the top of the stack if
	to the top of the stack if true.	true.
	Refer Elliptic Curve Digital Signature Algorithm (ECDSA)	
	HASH	
	= C2 - d * C1	
	$= C2 - PR_G * PU_B$	
	= 105 - 7 * 15	
	= <u>0</u>	
	1	