Problem 8. «Public keys for e-coins»

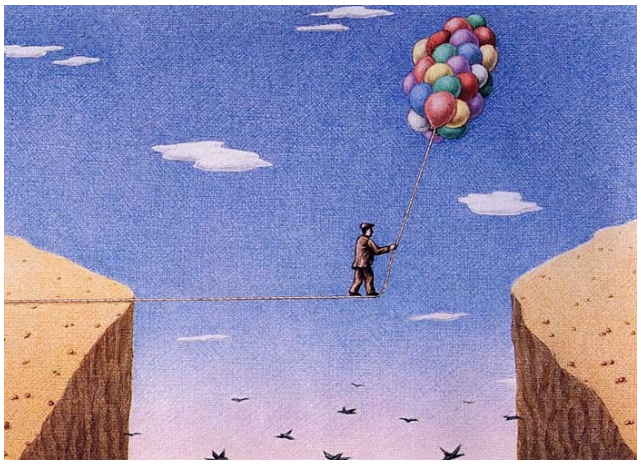
Alice has n electronic coins that she would like to spend via some public service S (bank). The service applies some asymmetric algorithm of encryption $E(,)$ and decryption $D(,)$ in its work. Namely, for the pair of public and private keys (PK, SK) and for any message m it holds: if $c = E(m, PK)$, then $m = D(c, SK)$ and visa versa: if $c' = E(m, SK)$, then $m = D(c', PK)$.

To spend her money, Alice generates a sequence of public and private key pairs $(PK_1, SK_1), \ldots, (PK_n, SK_n)$ and sends the sequence of public keys $PK_1, \ldots, PK_n$ to the service S. By this she authorizes the service S to control her n coins.

If Alice would like to spend a coin with number i in the shop of Bob, she just gives the secret key SK_i to Bob and informs him about the number i. To get the coin with number i, Bob sends to the service S three parameters: number i, some non secret message m, and its electronic signature $c' = E(m, SK_i)$. The service S checks whether the signature c' corresponds to the message m, i.e. does it hold the equality $m = D(c', PK_i)$. If it is so, the service accepts the signature, gives the coin number i to Bob and marks it as «spent».

Problem for a special prize! Propose a *modification of this scheme* related to generation of public and private key pairs. Namely, is it possible for Alice not to send the sequence of public keys $PK_1, \ldots PK_n$ to the service S, but send only some initial information enough for generating all necessary public keys on the service's side? Suppose that Alice sends to the service S only some initial key PK (denote it also as PK_0), some function f and a set of parameters T such that $PK_{i+1} = f(PK_i, T)$ for all $i \geqslant 0$. Propose your variant of this function f and the set T. Think also what asymmetric cryptosystem it is possible to use in such scheme.

Requirements to the solution. Knowing PK, f and T, it is impossible to find any private key SK_i, where $i = 1, \ldots, n$. It should be impossible to recover SK_i even if the secret keys $SK_1, \ldots, SK_{i-1}$ are also known, or even if all other secret keys are known (more strong condition).



The picture of Gürbüz Doğan Ekşioğlu.