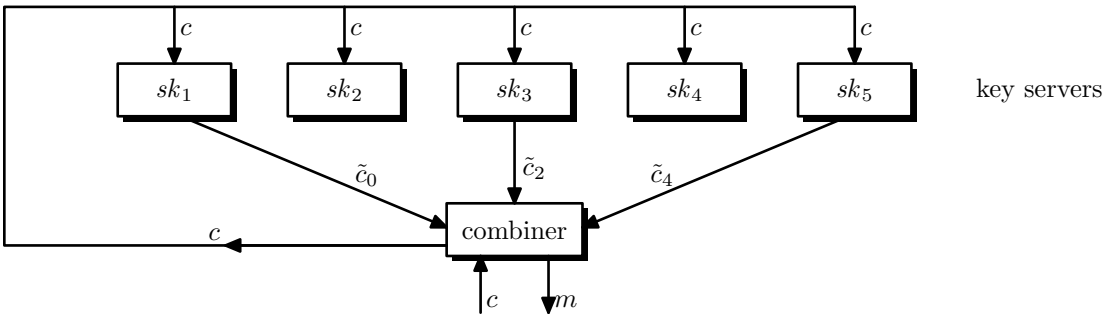

The combiner sends the given ciphertext c to all five key servers. Three servers respond, enabling the combiner to construct and output the plaintext message m.

Figure 11.5: Threshold decryption using three responses from five key servers.

---

sends back a "partial decryption." Once t responses are received from the key servers, the combiner can construct the complete decryption of c. The entire process is shown in Fig. 11.5. Overall, the system should decrypt c without reconstituting the key sk in a single location. Such a system is said to support threshold decryption.

Definition 11.6. *A* ***public-key threshold decryption scheme*** $\mathcal{E} = (G, E, D, C)$ *is a tuple of four efficient algorithms:*

- *G is a probabilistic algorithm that is invoked as $(pk, sk_1, \ldots, sk_s) \xleftarrow{R} G(s,t)$ to generate a t-out-of-s shared key. It outputs a public key pk and s shares $SK := \{sk_1, \ldots, sk_s\}$ of the decryption key.*
- *E is an encryption algorithm as in a public key encryption scheme, invoked as $c \xleftarrow{R} E(pk, m)$.*
- *D is a deterministic algorithm that is invoked as $c' \leftarrow D(sk_i, c)$, where sk_i is one of the key shares output by G, c is a ciphertext, and c' is a partial decryption of c using sk_i.*
- *C is a deterministic algorithm that is invoked as $m \leftarrow C(c, c'_1, \ldots, c'_t)$, where c is a ciphertext, and $c'_1, \ldots, c'_t$ are some t partial decryptions of c, computed using t distinct key shares.*
- *As usual, decryption should correctly decrypt well-formed ciphertexts; specifically, for all possible outputs $(pk, sk_1, \ldots, sk_s)$ of $G(s,t)$, all messages m, and all t-size subsets $\{sk'_1, \ldots, sk'_t\}$ of sk, for all outputs c of $E(pk, m)$, we have $C(\ c,\ D(sk'_1, c),\ \ldots,\ D(sk'_t, c)\ ) = m$.*

A public-key threshold decryption scheme is secure if an adversary that completely compromises $t-1$ of the key servers, and can eavesdrop on the output of the remaining key servers, cannot break semantic security. We will define security more precisely after we look at some constructions.

Note that Definition 11.6 requires that t and s be specified at key generation time. However, all the schemes in this section can be extended so that both t and s can be changed after the secret key shares are generated, without changing the public key pk.