TD 6 - Zero-knowledge protocol

1. ***Completeness***: *if Alice, who knows B, answers correctly, then we have;* $T' = D^v.J^d \mod n = (r.B^d)^v.J^d \mod n = r^v.(B^v.J)^d \mod n = r^v \mod n = T$.
Soundness: *if Eve, who doesn't know B, is correctly authenticated by Bob, then she has sent a correct couple* (T, D) *to Bob, with* D *v-root of* $T.J^{-d} \mod n$. *But she cannot compute v-root; thus the only way for Eve is to compute a couple* $(T,\ D)$ *verifying* $T = D^v.J^d$*, then such that* $J^d = D^v.T \mod n$*, also* $D^v.T = B^{-vd} \mod n$. *This may be possible for some values of d, for* $d = 0$ *for instance. But she does not know d; her only possibility is thus to bet on the value of d before sending T: she bets on d, chooses D and computes* $T = D^v.J^d \mod n$. *Her probability of success in correclty guessing d is only* $\frac{1}{v} \leq \frac{1}{2}$.

2. *For any value of d, we have to proove that the transcript* ($T = r^v \mod n; d; D = rB^d \mod n$) *gives no information on the secret key B.*

- *if* $d = 0$*: we have* $D = r \mod n$ *and* $T = r^v \mod n$. *So there is no information on B.*
- *id* $d = 1$*:* $T = r^v$ *and* $D = rB$*: due to assumption, T gives no knowledge on r; then knowing* $rB \mod n$ *gives no information on B.*
- *if* $d \geq 2$ *: Let* $B' = B^d \mod n$. *We have* $T = r^v \mod n$ *and* $D = r.B'$*; similarly to previous case, we have no information on* B' *except it is a v-power* $\mod n$. *But if we know B then we know* B' *by polynomial computation; so, by contradiction, if we do not know* B'*, we do not know B.*

3. *Bob takes the first* $\log_2 v$ *bits of* σ *and computes* $T' = D^v J^d \mod n$. *Then it computes* $d' = h(M||\ T')$. *The signature is verified iff* $d = d'$.