1

1.1

Removing preimage resistance has no effect. If we are trying to forge a signature for a message, we already have it, and we don't need to deduce it from the hash.

1.2

Removing 2nd-preimage resistance leads to an EF under CMA, as follows: as our hash fails 2nd-preimage resistance, suppose that given some message x, we can easily find a message y such that $h(x) = h(y)$, where h is the hash. Then, if we can convince the signer to sign the message x, it's signature will coincide will the signature for y. This provides the forgery. This attack is not adaptive.

1.3

Removing collision resistance leads to an EF under CMA. This is the same attack as the previous one, just on the pair x, y that invalidates collision resistance.

2

2.1

Proof: If the signature is valid, then: $r \equiv g^k (\mathrm{mod} p)^s \equiv (m - xr)k^{-1} (\mathrm{mod} p - 1)$ Now:

- as $1 < g < p$, and as $\{1, 2, ..., p - 1\}$ is closed under multiplication modulo p (as p is prime), inductively, $r \equiv g^k \not\equiv 0$.