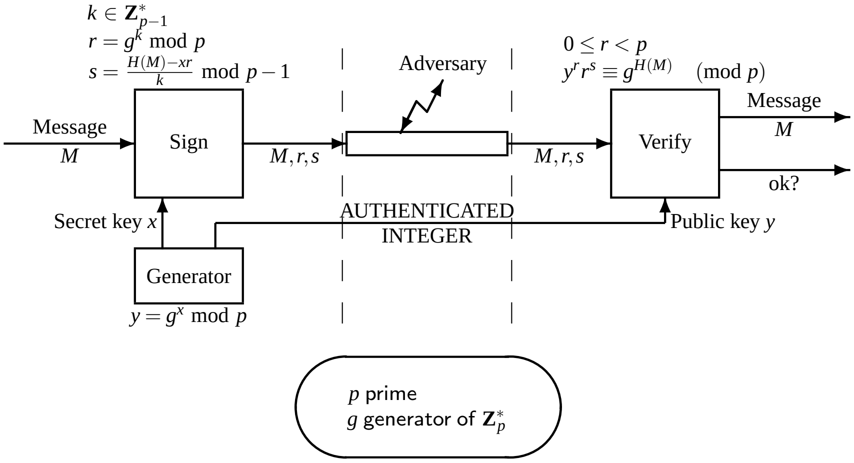
ElGamal Signature

(Below is a copy of the ElGamal digital signature scheme slide from the course.)

1. Tell one typical application for digital signatures.
2. Explain how to generate public parameters.
3. Explain how to generate a key pair.
4. Explain why signatures generated from the Sign algorithm pass the Verify test.
5. What is the security of the scheme with respect to key recovery?
6. What is the security of the scheme with respect to existential forgeries?
7. What happens if the $0 \leq r < p$ test is omitted in the Verify test?
8. Suggest some parameter lengths and H instance for practical use. What is the signature length?
9. How to shrink it?
10. Mention a known security problem in the ElGamal signature scheme.


$k \in \mathbf{Z}_{p-1}^*$
$r = g^k \bmod p$
$s = \frac{H(M)-xr}{k} \bmod p-1$
Adversary
$0 \leq r < p$
$y^r r^s \equiv g^{H(M)} \pmod{p}$
Message
M
Sign
M, r, s
M, r, s
Verify
Message
M
ok?
Secret key x
AUTHENTICATED
INTEGER
Public key y
Generator
$y = g^x \bmod p$
p prime
g generator of $\mathbf{Z}_p^*$