El Gamal Signature scheme

Assume that Alice has an El-Gamal key for which the public part is \((g, b, P)\), and the private part is the number \(a\). Recall:

- \(P\) is a prime number.
- \(1 < g < P\) is a primitive root of \(P\).
- \(b = g^a \mod P\).

Typically there would also be a hash-function \(H\) involved in digitally signing a message \(M\) with an El-Gamal signature. One would first compute \(H(M)\), the hash of the message, and then digitally sign the hash. For purposes of exposition, we may denote the quantity (whether it be the hash or just the raw message) which will be signed also by \(M\). The \(M\) we sign must be less than \(P\). We describe here how a message \(M\) would be signed, assuming that \(M < P\).

**Signature algorithm**

- Select randomly a number \(r < P - 1\) such that \(\gcd(r, P-1) = 1\).
- Compute \(y = g^r \mod P\).
- Compute \(s = (M - a^y)(r^{-1}) \mod (P - 1)\).

Alice’s El-Gamal signature on \(M\) is \((y, s)\).

**Verification algorithm**

The verifier knows the following things: Alice’s public key \((g, b, P)\), the message \(M\) and presented signature \((y, s)\). The verifier does NOT know Alice’s private key \(A\) and the random number \(r\) chosen by Alice.

The verifier now computes:

- \(V_1 = y^s \cdot b^y \mod P\).
- \(V_2 = g^M \mod P\).

If \(V_1 = V_2\), and if \(y, s < P\), then the signature \((y, s)\) is accepted as Alice’s; otherwise, the signature is not accepted.