

Algorithms

EXTENDED EUCLIDEAN ALGORITHM (a, b)

- $s_0 = 1, s_1 = 0, t_0 = 0, t_1 = 1$.
- Compute $r_{i-2} = r_{i-1}q_{i-1} + r_i$ and $s_i = s_{i-2} - q_{i-1}s_{i-1}, t_i = t_{i-2} - q_{i-1}t_{i-1}$ as long as $r_i > 0$.

SOLOVAY-STRASSEN(n)

- Select a random integer a with $1 \leq a \leq n - 1$ and compute $x := \left(\frac{a}{n}\right)$. (How?)
- If $x = 0$ then return "composite". (Why is this step correct?)
- Compute $y := a^{(n-1)/2} \bmod n$. (How?)
- Check if $x \equiv y \pmod n$. If yes then return "prime" else return "composite".

MILLER-RABIN(n)

- First find m, k so that $n - 1 = 2^k m$ and m is odd.
- Choose a random integer a with $1 \leq a \leq n - 1$ and compute $b := a^m \bmod n$. (How?)
- If $b \equiv 1 \pmod n$ return "prime".
- Iterate k times: (a) if $b \equiv -1 \pmod n$ return "prime" (b) $b := b^2 \pmod n$.
- return "composite".

POLLARD ALGORITHM(n, B)

- Compute $a := 2^{B!} \bmod n$. (How?)
- Find $d = \gcd(a - 1, n)$ and if $1 < d < n$ return d else return "fail".

Proofs

1. **Number of keys in the affine cipher:** Show $x \rightarrow ax + b$ is injective if and only if $\gcd(a, m) = 1$.
2. **Size of Z_m^* :** Show that a has an inverse if and only if $x \rightarrow ax$ is injective.
3. **Characterization of perfect secrecy:**
 - For the forward implication, first note that $|\mathcal{C}| = |\mathcal{K}|$ gives $|\{e_K(x) | K \in \mathcal{K}\}| = |\mathcal{K}|$ and so $e_{K_1}(x) \neq e_{K_2}(x)$ when $K_1 \neq K_2$.
 - Then conclude that for every x, y there is unique K such that $e_K(x) = y$.
 - Now fix y and use Bayes' Theorem to argue $\Pr[K_i] = \Pr[y|x_i] = \Pr[y]$
 - For the backward implication, compute $\Pr[y], \Pr[y|x]$ and apply the Bayes' Theorem.
4. **Key equivocation $H(K|C) = H(K) + H(P) - H(C)$:** Compute $H(K, P, C)$ in two different ways: (1) $H(C|K, P) + H(K, P) = H(K) + H(P)$ (2) $H(P|K, C) + H(K, C) = H(K|C) + H(C)$.
5. **Lagrange Theorem:** Consider $H = \{h^i | i = 0 \dots m\}$ with m order of h in G and show that sets $aH = \{ah^i | i = 0 \dots m\}$ partition G .
6. **Fermat Theorem:** If p does not divide b then $b \in Z_p^*$ and its order must divide $p - 1$.
7. **RSA:** Use $\phi(n) = (p - 1)(q - 1)$ and note that $ab = \phi(n)l + 1$. Observe that $d_K(e_K(x)) \equiv x \pmod{p}$ and $d_K(e_K(x)) \equiv x \pmod{q}$ by using Fermat Theorem. Now invoke the uniqueness of CRT to claim $d_K(e_K(x)) \equiv x \pmod{n}$.
8. **Euler's Criterion:** For the forward implication, use the Fermat Theorem. For the converse, use a primitive elements α giving $a = \alpha^i$ and argue that i must be even by using the fact $\alpha^k \equiv 1 \pmod{p}$ gives $(p - 1) | k$.

9. **Solovay-Strassen:** This is based on the fact that if p is prime then $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right)$ which follows from Euler's Theorem.
10. **Miller-Rabin:** Assume n is prime and the answer is "composite". Then all a^{m2^i} with $i = 0, \dots, k-1$ are not congruent to $-1 \pmod n$. From Fermat's Theorem $a^{m2^k} \equiv 1 \pmod n$ which gives $a^{m2^i} \equiv 1 \pmod n$ by going down with $i = k, \dots, 0$. Thus $a^m \equiv 1 \pmod n$ which contradicts step 3.
11. **Pollard's $p-1$ algorithm:** Let p with $p|n$ be a prime number. Suppose that $(p-1)|B!$. Since $a = 2^{B!} \pmod n$, $a \equiv 2^{B!} \pmod p$ and so from Fermat $a \equiv 1 \pmod p$. Thus $p|(a-1)$.