Exercise 8 in Cryptography
- Proposed Solution -

Prof. Dr. Rudolf Mathar, Henning Maier, Jose Angel Leon Calvo

2015-06-25

Solution of Problem 24

Let $\varphi : \mathbb{N} \to \mathbb{N}$ the Euler φ-function, i.e., $\varphi(n) = |\mathbb{Z}_n^*|$ with $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid \gcd(a, n) = 1\}$.

a) Let $n = p$ be prime. It follows for the multiplicative group that:

$$\mathbb{Z}_p^* = \{a \in \mathbb{Z}_p \mid \gcd(a, p) = 1\} = \{1, 2, \dots, p-1\} \Rightarrow \varphi(p) = p - 1\,.$$

b) The power p^k has only one prime factor. So p^k has a common divisors that are not equal to one: These are only the multiples of p. For $1 \le a \le p^k$:

$$1 \cdot p\,, \quad 2 \cdot p\,, \quad \dots\,, \quad p^{k-1} \cdot p = p^k\,.$$

And it follows that

$$\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)\,.$$

c) Let $n = p\,q$ for two primes $p \neq q$. It holds for $1 \le a < p\,q$

1) $p \mid a \vee q \mid a \Rightarrow \gcd(a, p\,q) > 1$, and
2) $p \nmid a \wedge q \nmid a \Rightarrow \gcd(a, p\,q) = 1$.

It follows $\mathbb{Z}_{p\,q}^* = \underbrace{\{1 \le a \le p\,q - 1\}}_{p\,q-1 \text{ elements}} \setminus \left[\underbrace{\{1 \le a \le p\,q - 1 \mid p \mid a\}}_{q-1 \text{ elements}} \,\dot\cup\, \underbrace{\{1 \le a \le p\,q - 1 \mid q \mid a\}}_{p-1 \text{ elements}}\right]$.

Hence: $\varphi(p\,q) = (p\,q-1)-(q-1)-(p-1) = p\,q-p-q+1 = (p-1)(q-1) = \varphi(p)\,\varphi(q)$.

d) Apply the Euler phi-function on n with the following steps:

1. Factorize all prime factors of the given n
2. Apply the rules in a) to c), correspondingly.

$\varphi(4913) = \varphi(17^3) \overset{(b)}{=} 17^2(17-1) = 4624$, and
$\varphi(899) = \varphi(30^2 - 1^2) = \varphi((30-1)(30+1)) = \varphi(29 \cdot 31) \overset{(c)}{=} 28 \cdot 30 = 840$.

Solution of Problem 25

a) Define event A : 'n composite' $\Leftrightarrow \bar{A}$: 'n prime'.
Define event B : m-fold MRPT provides 'n prime' in all m cases.
From hint: $\text{Prob}(\bar{A}) = \frac{2}{\ln(N)} \Rightarrow \text{Prob}(A) = 1 - \frac{2}{\ln(N)}$ (cf. Thm. 6.7)

Probability for the case that the MRPT fails for m times:

$$\text{Prob}(B \mid A) \leq \left(\frac{1}{4}\right)^m$$

Probability of the MRPT verifying an actual prime is:

$$\text{Prob}(B \mid \bar{A}) = 1$$

Probability of the MRPT wrongly verifying a composite n as prime after m tests is:

$$\begin{aligned}
p &= \text{Prob}(A \mid B) \\
&= \frac{\text{Prob}(B \mid A) \cdot \text{Prob}(A)}{\text{Prob}(B)} \\
&= \frac{\text{Prob}(B \mid A) \cdot \text{Prob}(A)}{\text{Prob}(B \mid A) \cdot \text{Prob}(A) + \text{Prob}(B \mid \bar{A}) \cdot \text{Prob}(\bar{A})} \\
&\leq \frac{(\frac{1}{4})^m (1 - \frac{2}{\ln(N)})}{(\frac{1}{4})^m (1 - \frac{2}{\ln(N)}) + 1 \cdot \frac{2}{\ln(N)}} \\
&= \frac{\ln(N) - 2}{\ln(N) - 2 + 2^{2m+1}}
\end{aligned}$$

b) Note that the above function $f(x) = \frac{x}{x+a}$ is monotonically increasing for $x \in \mathbb{R}$, $a > 0$, as its derivative is $f'(x) = \frac{a}{(x+a)^2} > 0$. Let $x = \ln(N) - 2$, and $N = 2^{512}$.
Resolve the inequality w.r.t. m:

$$\begin{aligned}
\frac{x}{x + 2^{2m+1}} &< \frac{1}{1000} \\
\Leftrightarrow 2^{2m+1} &> 999x \\
\Leftrightarrow m &> \tfrac{1}{2}(\log_2(999x) - 1) \\
\Leftrightarrow m &> \tfrac{1}{2}(\log_2(999(512\ln(2) - 2)) - 1) \\
\Leftrightarrow m &> 8.714.
\end{aligned}$$

$m = 9$ repetitions are needed to ensure that the error probability stays below $p = \frac{1}{1000}$ for $N = 2^{512}$.

Solution of Problem 26

a) Let n be odd and composite. The problem is modelled by a geometric distributed random variable X with:

- Probability of a single test stating 'n is prime' although n is composite is p ($\Rightarrow 1-p$ for 'n is composite')
- Probability that after exactly $M \in \mathbb{N}$ tests, it correctly states 'p is composite':

$$\mathrm{Prob}(X = M) = p^{M-1}(1-p)$$

b) The expected value of a geometrically distributed random variable is:

$$\mathsf{E}(X) = \sum_{M=1}^{\infty} M p^{M-1}(1-p) = (1-p)\frac{p}{(1-p)^2} = \frac{p}{1-p},$$

Note that with the geometric series $\sum_{n=0}^{\infty} x^n = \frac{1}{1-x}$, we can compute its derivative w.r.t. x, and obtain $\sum_{n=1}^{\infty} n x^{n-1} = \frac{x}{(1-x)^2}$, for $|x| < 1$.

For the given parameter $p = \frac{1}{4}$, the expected value for the number of tests stating that a composite n is indeed composite is:

$$\mathsf{E}(X) = \frac{p}{1-p} = \frac{1/4}{1-1/4} = \frac{1/4}{3/4} = \frac{1}{3}$$

Solution of Problem 27

a) "$\Rightarrow$" Let n with $n > 1$ be prime. Then, each factor m of $(n-1)!$ is in the multiplicative group $\mathbb{Z}_n^*$. Each factor m has a multiplicative inverse modulo n. The factors 1 and $n-1$ are obviously inverse to themselves. The factorial multiplies all these factors. The entire product must be 1 since all pairs of inverses yield 1.

$$(n-1)! \equiv \prod_{i=1}^{n-1} i \equiv \underbrace{(n-1)}_{\text{self-inv.}} \underbrace{(n-2)\cdot \ldots \cdot 3 \cdot 2}_{\text{pairs of inv. } \equiv 1} \cdot \underbrace{1}_{\text{self-inv.}} \equiv (n-1) \equiv -1 \mod n$$

"$\Leftarrow$" Let $n = ab$ and hence composite with $a, b \neq 1$ prime. Thus $a|n$ and $a|(n-1)!$. From $(n-1)! \equiv -1 \Rightarrow (n-1)! + 1 \equiv 0$, we obtain $a|((n-1)!+1) \Rightarrow a|1$ $\Rightarrow a = 1 \Rightarrow n$ must be prime. ↯

b) Compute the factorial of 28:

$$\begin{aligned}28! &= \overbrace{(28\cdot 27)}^{2}\cdot\overbrace{(26\cdot 25)}^{12}\cdot\overbrace{(24\cdot 23)}^{1}\cdot\overbrace{(22\cdot 21)}^{27}\cdot\overbrace{(20\cdot 19)}^{3}\cdot\overbrace{(18\cdot 17)}^{16}\\ &\quad \underbrace{(16\cdot 15)}_{8}\cdot\underbrace{(14\cdot 13)}_{8}\cdot\underbrace{(12\cdot 11)}_{16}\cdot\underbrace{(10\cdot 9\cdot 8)}_{24}\cdot\underbrace{(7\cdot 6\cdot 5\cdot 4)}_{28}\cdot\underbrace{(3\cdot 2)}_{6}\\ &= \underbrace{(2\cdot 12\cdot 1\cdot 27\cdot 3)}_{1}\cdot\underbrace{(16\cdot 8\cdot 8\cdot 16)}_{-1}\cdot\underbrace{(24\cdot 28\cdot 6)}_{1} \equiv -1 \mod 29\end{aligned}$$

Thus, 29 is prime as shown by Wilson's primality criterion.

c) Using this criterion is computationally inefficient, since computing the factorial is very time-consuming.