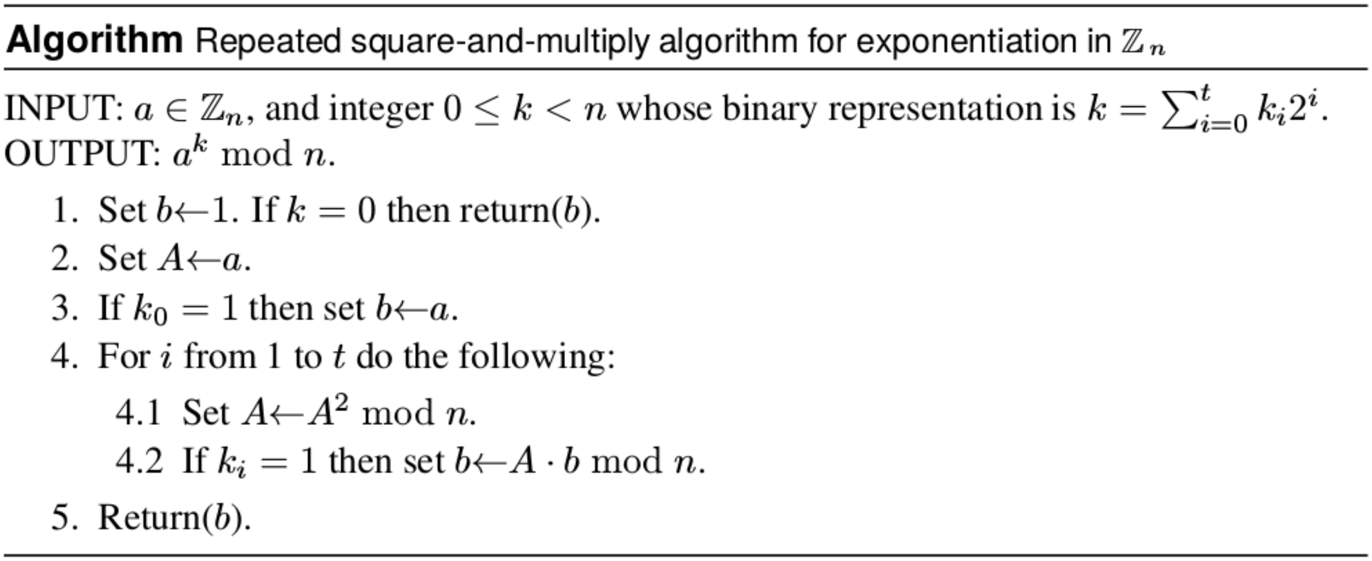
23rd Aug, 2016

Security Lab

Assignment

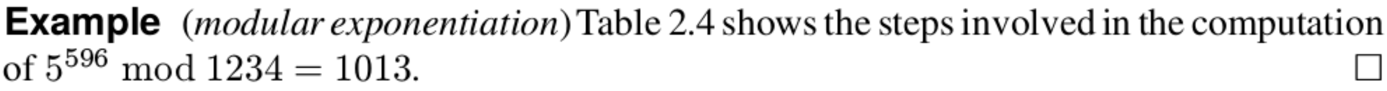
Square-and-Multiply Method for Modular Exponentiation with example



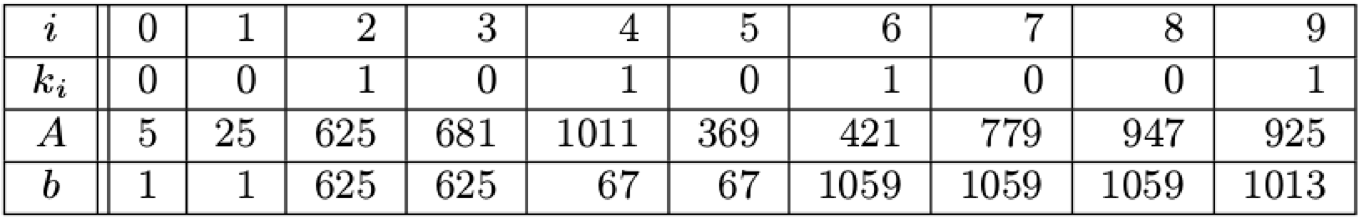
Algorithm Repeated square-and-multiply algorithm for exponentiation in $\mathbb{Z}_n$

INPUT: $a \in \mathbb{Z}_n$, and integer $0 \leq k < n$ whose binary representation is $k = \sum_{i=0}^{t} k_i 2^i$.
OUTPUT: $a^k \bmod n$.

```
1. Set $b \leftarrow 1$. If $k = 0$ then return($b$).
2. Set $A \leftarrow a$.
3. If $k_0 = 1$ then set $b \leftarrow a$.
4. For $i$ from 1 to $t$ do the following:
    4.1 Set $A \leftarrow A^2 \bmod n$.
    4.2 If $k_i = 1$ then set $b \leftarrow A \cdot b \bmod n$.
5. Return($b$).
```



Example (*modular exponentiation*) Table 2.4 shows the steps involved in the computation of $5^{596} \bmod 1234 = 1013$. □



i	0	1	2	3	4	5	6	7	8	9
k_i	0	0	1	0	1	0	1	0	0	1
A	5	25	625	681	1011	369	421	779	947	925
b	1	1	625	625	67	67	1059	1059	1059	1013