./SeptDec2015/Lesson19RSA/Lesson19RSA.sagews

November 18, 2015

Bob wants to send Alice a secure message using RSA.

Alice chooses a public key (e, n) satisfying $n = pq$ for distinct primes p and q and e is a positive integer satisfying $\gcd(e, (p-1)(q-1)) = 1$.

```
p = next_prime(12345); print(p);
q = next_prime(54321); print(q);
n = p*q; print(n);
e = 17; print(e, gcd(e,(p-1)*(q-1)));
```

```
12347
54323
670726081
(17, 1)
```

Alice publishes (e, n)

Bob wants to send his message M, an integer strictly between 1 and n.

Bob computes $C \equiv M^e \mod n$ with $0 < C < n$.

```
M = 11111111
C = power_mod(M,e,n); print(C)
```

```
512017456
```

Bob sends C to Alice.

Alice receives C and computes d such that $ed \equiv 1 \mod (p-1)(q-1)$.

```
d = power_mod(e,-1,(p-1)*(q-1)); print(d)
```

```
118351661
```

Alice now computes $R \equiv C^d \mod n$.

```
R = power_mod(C,d,n); print(R)
```

```
11111111
```