

# Lecture 32: Factorization & RSA Assumptions

- In the previous lectures we have seen how to generate a random  $n$ -bit prime number
- We also saw how to efficiently test whether a number is a prime number or a composite number (basic Miller–Rabin Test)

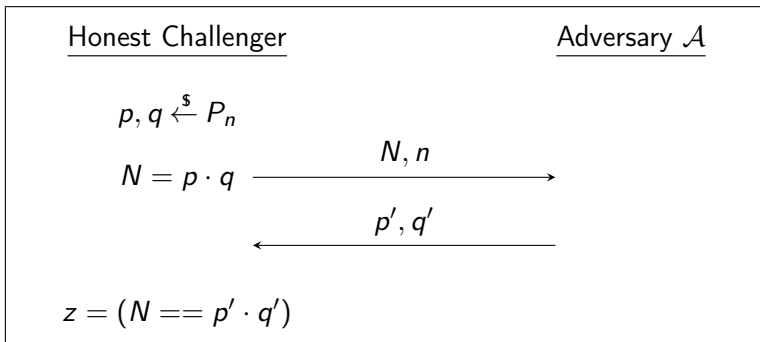
- Today we will see two new computational hardness assumptions: Hardness of Factorization and the RSA Assumption

# Hardness of Factorization I

- The hardness of factorization, intuitively, states the following:  
Any computational adversary given as input  $N$ , the product of two random  $n$ -bit prime numbers, shall not be able to factor it (except with exponentially low probability)

# Hardness of Factorization II

- Formally, consider the following experiment. Let  $P_n$  represent the set of all primes that need  $n$ -bits in their binary representation.



- Hardness of Factorization Assumption.** For all computationally efficient adversaries  $\mathcal{A}$ , the probability of  $z = 1$  is exponentially small in  $n$

## Notes.

- There might be bad primes for which it is easy to factorize  $N$ . But this assumption states that it is hard to factorize when  $p, q$  are picked uniformly at random from  $P_n$
- The (decision version of the) factorization problem is conjectured to a problem that lies in  $NP \setminus P$  (i.e., outside  $P$  but in  $NP$ ) and is not  $NP$ -complete

# RSA Assumption I

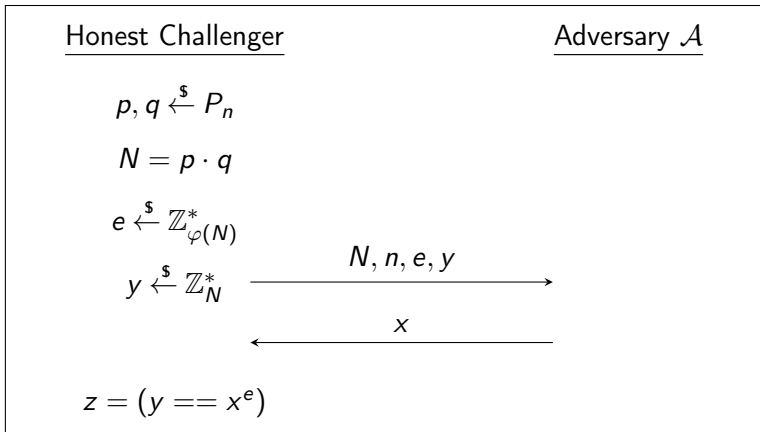
- Let  $N$  be the product of two  $n$ -bit primes numbers  $p, q$  chosen uniformly at random from the set  $P_n$
- Let  $\varphi(N) = (p - 1)(q - 1)$  be the number of elements in  $\mathbb{Z}_N^*$  (the set of integers that are relatively prime to  $N$ )
- We shall state the following result without proof

## Claim

*Let  $e \in \{1, 2, \dots, \varphi(N) - 1\}$  be any integer that is relatively prime to  $\varphi(N)$ . Then, the function  $x^e$  from the domain  $\mathbb{Z}_N^*$  to the range  $\mathbb{Z}_N^*$  is a bijection.*

## RSA Assumption II

- The RSA Assumption states the following.



- RSA Assumption.** For any computationally bounded adversary  $\mathcal{A}$ , the probability that  $z = 1$  is exponentially small



# RSA Assumption: Worked-out Example I

- Suppose  $N = 3 \cdot 11 = 33$
- Then, we have  $\varphi(N) = 2 \cdot 10 = 20$
- Note that  $\mathbb{Z}_N^* = \{1, 2, 4, 5, 7, 8, 10, 13, 14, 16, 17, 19, 20, 23, 25, 26, 28, 29, 31, 32\}$
- Suppose  $e = 3$
- Let  $d$  be such that  $e \cdot d = 1 \pmod{\varphi(N)}$ . So, we have  $d = 7$

# RSA Assumption: Worked-out Example II

First, we want to show that  $x^e$  is a bijection from the domain  $\mathbb{Z}_N^*$  to the range  $\mathbb{Z}_N^*$

Then, we want to show that, given  $d$ , we can find  $y^{1/e}$  efficiently

$x$	1	2	4	5	7	8	10	13	14	16	17	19	20	23	25	26	28	29	31	32
$x^2$	1	4	16	25	16	31	1	4	31	25	25	31	4	1	31	16	25	16	4	1
$y = x^e = x^3$	1	8	31	26	13	17	10	19	5	4	29	28	14	23	16	20	7	2	25	32
$x^4$	1	16	25	31	25	4	1	16	4	31	31	4	16	1	4	25	31	25	16	1
$x^d = x^7$	1	29	16	14	28	2	10	7	20	25	8	13	26	23	31	5	19	17	4	32
$y^7$	1	2	4	5	7	8	10	13	14	16	17	19	20	23	25	26	28	29	31	32