University of Michigan–Ann Arbor

Department of Electrical Engineering and Computer Science

EECS 475 **Introduction to Cryptography**, Winter 2023

Lecture 24: Digital Signatures, Modeling Digital Signatures, RSA Signatures

April 5, 2023

Lecturer: Mahdi Cheraghchi

Scribe: Yi-Wen Tseng

1 Continue on Better RSA Encryption Approach

Apply $RSA_{N,e}$ on a random $x \leftarrow \mathbf{Z}_N^*$. Then, we know x is hard to recover from $y = RSA_{N,e}(x)$. We first use a hash function on x and encrypt message m:

$$c = (y = RSA_{N,e}(x) = x^e \bmod N, H(x) \oplus m)$$

$Dec(sk = (N, d), c = (y, p))$: Compute $x = RSA_{N,d}(y) = y^d \bmod N$ and output $H(x) \oplus p$. This mechanism meets the correctness requirement.
Note: Because x is unknown, $H(x)$ would be close to completely unknown.

We also need to check security requirement of RSA.

CPA Security: Hash function (really random like)
A good hash function "practically behaves" like a uniform random function (a.k.a random oracle) e.g.

2 Digital Signature

3 Modeling Digital Signature

4 RSA Signature