# Digital signatures

Alice $\xrightarrow{m}$ Bob
$(s)$ signature for $m$

goals:
- integrity
- authenticity ("proof that $(m,s)$ is from A")

RSA signatures · $H$ collision-resistant hash

- A: public RSA key $(N, e)$
  private key $d$
- A's signature of $m$:
  $s \equiv H(m)^d \pmod N$
- To verify signed message $(m,s)$
  $H(m) \stackrel{?}{\equiv} s^e \pmod N$

review:
encrypt: $c \equiv m^e \pmod N$
decrypt: $m \equiv c^d \pmod N$

Eve: knows $(m,s)$, $H(m)$
knows $s$ encrypts to $H(m)$

⇝ RSA signatures secure if RSA is secure against known plaintext attacks

EG $H(x) \equiv x \pmod{10}$ silly
Alice's public key: $(N,e) = (33, 3)$
private key: $d = 7$

(a) How does A sign $m = 12345$?
$s \equiv H(m)^d \pmod N$
$5^7 \pmod{33} \equiv 14$

(b) Did A sign $(m,s) = (314, 2)$?
$H(m) \stackrel{?}{\equiv} s^e \pmod N$
$4 \neq 2^3 = 8 \pmod{33}$ NO