# Xi Liu, Assignment 4

1

let the message be $m$, ciphertext be $c$, public key be $< n, e >$, private key be $< n, d >$

$$\begin{aligned} c &:\equiv m^e \mod n \\ c' &:\equiv (2m)^e \equiv 2^e m^e \equiv 2^e c \mod n \end{aligned}$$

Trudy can send $c' = 2^e c \mod n$ to Alice

2

2 or more signatures from the signer are required to forge a signature

$$\begin{aligned} &m, m_1 \in \mathbb{Z}^* \\ &\quad m_2 := m/m_1 \mod n \\ &\quad \sigma := \sigma_1 \sigma_2 \mod n \\ &\quad \sigma^e = (\sigma_1 \sigma_2)^e = (m_1^d m_2^d)^e = m_1^{ed} m_2^{ed} = m_1 m_2 = m \mod n \end{aligned}$$

$\sigma$ is a valid signature since $\sigma_1, \sigma_2$ are valid signatures. this is a forgery since $m \neq m_1$, $m \neq m_2$

3

this is hiding since based on the Decisional Diffie Hellman assumption and hardness of discrete logarithm problem, it is hard to compute $a, b$ from knowing only $g$ and $m \cdot g^{ab}$. it is binding since $g^{ab}$ is sent to the receiver first, the sender cannot change the copy that was sent to the receiver before sending $a$ and $b$

4

if Bob has a way to change his bit $b_1$ after seeing Alice opening her $b_0$, then this is insecure

a better way is for Alice to send $com(b_0)$ to Bob first, then Bob send his $b_1$ to Alice, then Alice opens $b_0$, in this way the integrity of $b_0$ is ensured