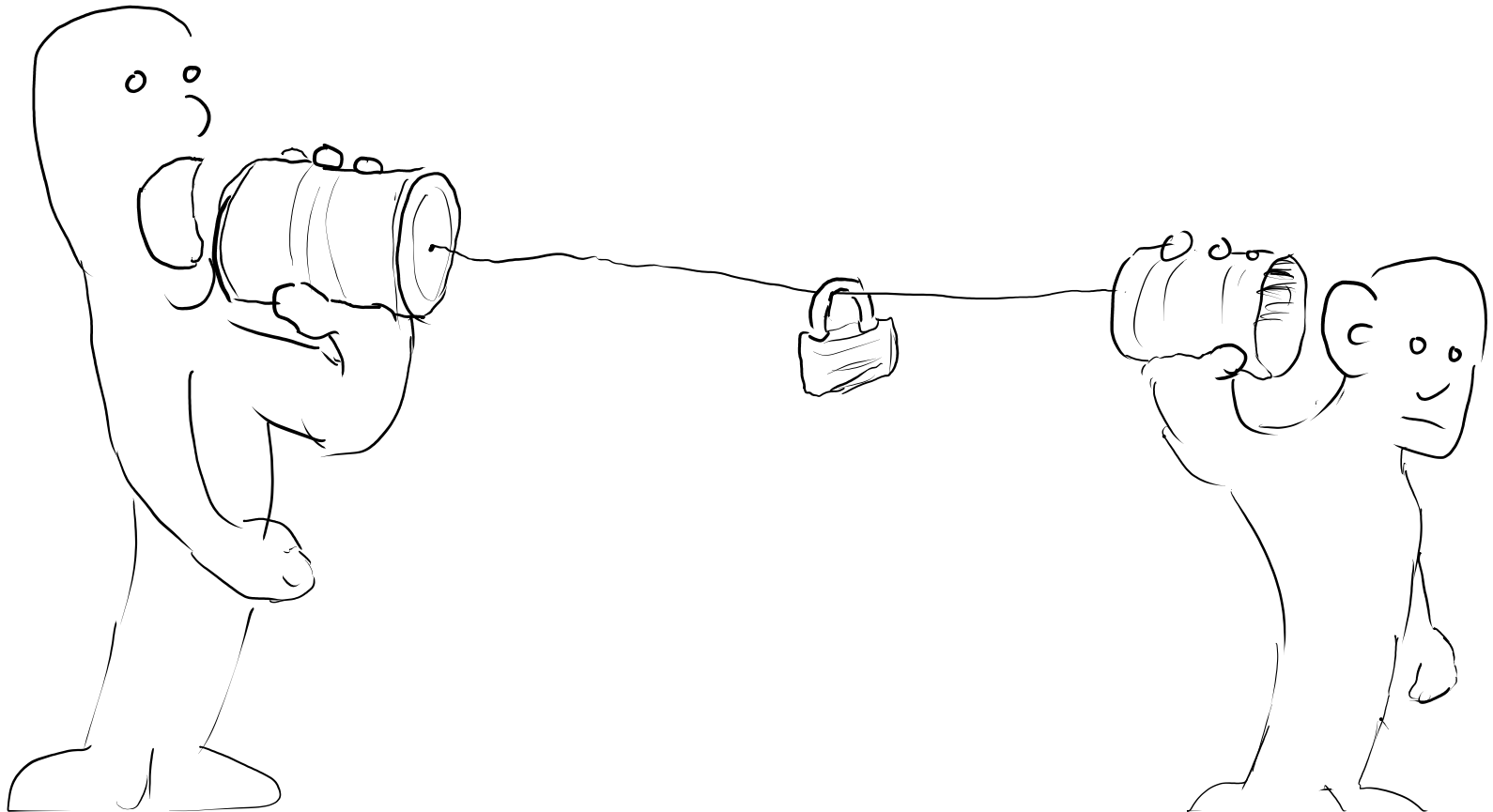


Hash

in: any thing (any number of bytes)

out: Fixed-size value = 20 bytes
= 50-digit number
= 20-character string (text)
= ....

Property: similar input has different output

hard to find input that gives specific output

---

fingerprint

Symmetric cipher ((ode)

in: 1. message (any text or bytes)

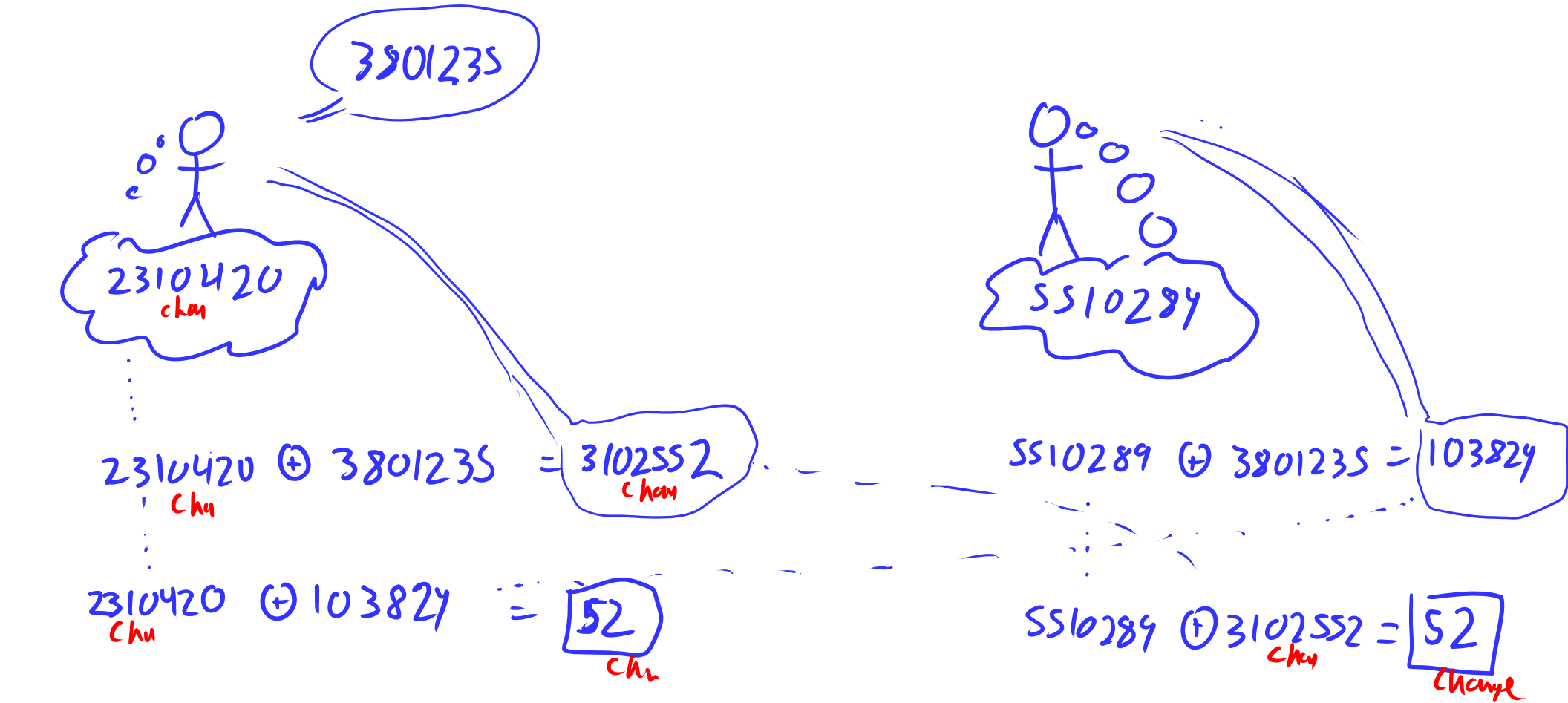
2. key (secret number or small value)

out: different message

encode : in "plaintext" message out: "ciphertext" message (nonsense)

decode : in "ciphertext" out: "plaintext"

Merkle - Diffie - Hellman key exchange



Signature

in:
1. message
2. private key — never tell anyone
3. public key — identity

out: encrypted hash

Check Signature

in:
1. message
2. public key
3. signature

out: decrypt(sig) $\stackrel{?}{=}$ hash(message)