

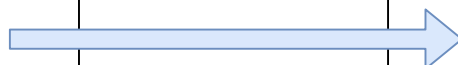
①公開鍵を配布



秘密鍵



公開鍵



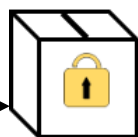
②データをハッシュ化



ha0sh1

③秘密鍵を使って暗号化

ha0sh1



④暗号化データと
元のデータを送信



公開鍵

⑤データを
ハッシュ化



ha0sh1

⑥暗号化データ
の復号



ha0sh1

ha0sh1

⑦データの比較

ha0sh1

ha0sh1

一致

正しいデータであることを確認