高等学校「情報I」対策講座

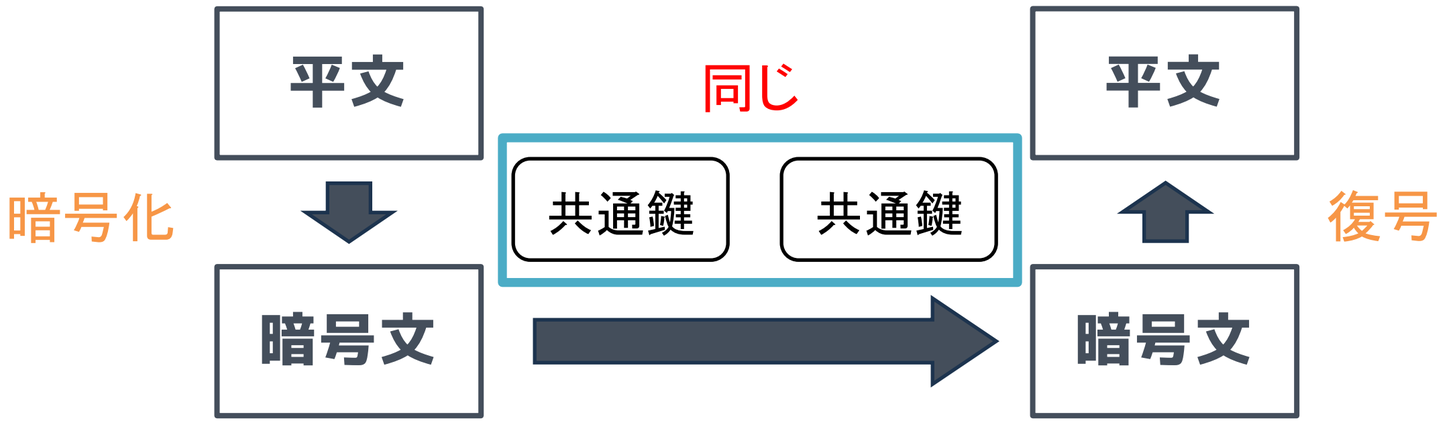
セキュリティ

暗号化方式
デジタル署名

共通暗号方式

暗号化に使う鍵と復号に使う鍵が同じ方式

◆平文　…　暗号化されていないデータ
◆暗号文…　暗号化されたデータ
◆復号　…　暗号文を平文に戻すこと



共通暗号方式

暗号化に使う鍵と復号に使う鍵が同じ方式

◆シーザー暗号　…　アルファベット順に決められた数だけ右にずらし，
元に戻すときは左にズラすだけ

平文：　ABCDEFGHIJKLMNOPQRSTU

暗号文：　ABCDEFGHIJKLMNOPQRSTU

共通鍵

Y＝x＋4

公開鍵暗号方式

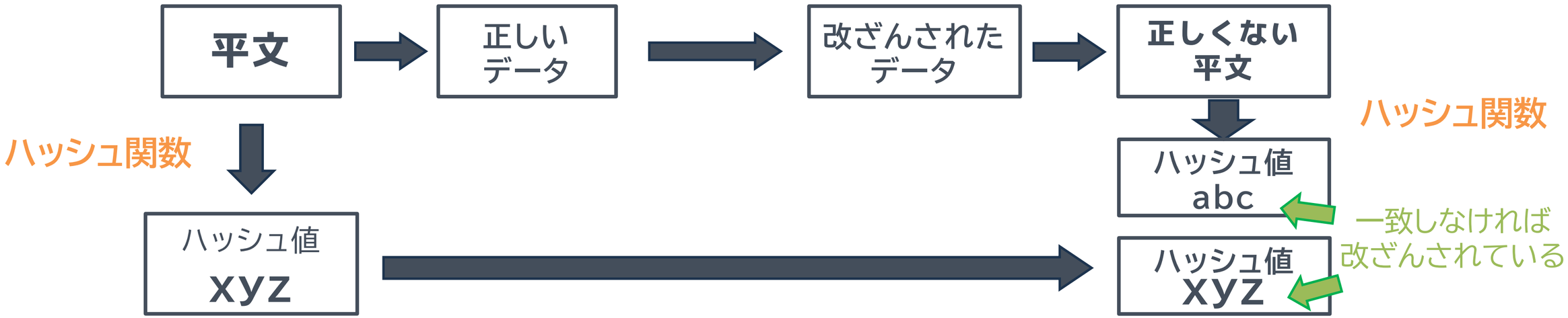
送信されたデータが間違いなく本人（送信者）のものである，つまり，改ざんされていないことが証明できる

◆秘密鍵　…　鍵を発行した本人以外に漏らしてはいけない情報
◆公開鍵　…　第三者に知られてもよい情報

ハッシュ値・ハッシュ関数

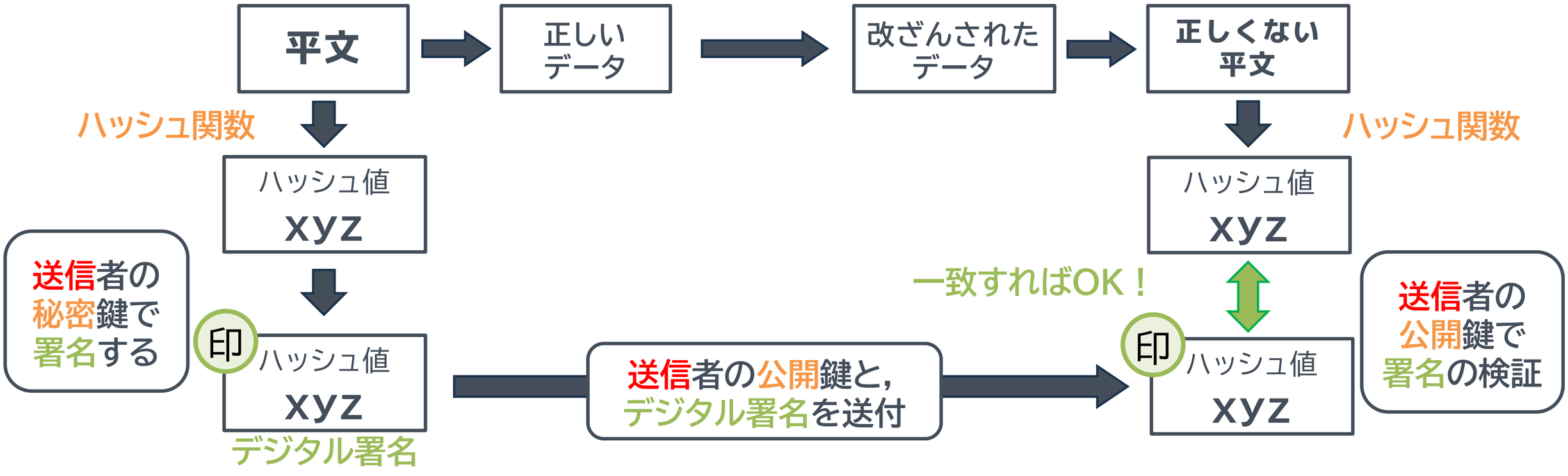
元のデータをハッシュ関数で，ハッシュ値(要約文)にする

◆ハッシュ関数　…　データを元に戻すことが困難状態にする関数
◆ハッシュ値（要約文）　…　関数にデータを代入して，出力される値



デジタル署名

送信されたデータが間違いなく本人（送信者）のものである，つまり，改ざんされていないことが証明できる



共通鍵暗号方式と公開鍵暗号方式

送信されたデータが間違いなく本人（送信者）のものである，つまり，改ざんされていないことが証明できる

正しいものを選べ.

① 公開鍵暗号方式は，共通鍵暗号方式より処理速度が遅い

② 10人以上が使用する場合，共通鍵暗号方式の方が公開鍵暗号方式より鍵の数は少なくてすむ

③ 鍵の受け渡しは，共通鍵暗号方式は送信者に鍵を渡すが，公開鍵暗号方式は送信者に渡す鍵と渡さない鍵がある

共通鍵暗号方式と公開鍵暗号方式

送信されたデータが間違いなく本人（送信者）のものである，つまり，改ざんされていないことが証明できる

解答

① 処理速度は，速い：共通鍵暗号方式　遅い：公開鍵暗号方式

② 10人の場合，共通鍵暗号方式は，${}_{10}C_2=45$本　多い
公開鍵暗号方式は，$2\times10=20$本　少ない

③ 鍵の受け渡しは，
共通鍵暗号方式　→　送信者に鍵を渡す
公開鍵暗号方式　→　送信者に渡す鍵と渡さない鍵（秘密鍵）がある