

暗号化について

3年 情報

今日の流れ

2

① 1年次のプリントを見ながら用語確認 (15分)

☆少し丁寧に確認

② 基本情報、全統模試 (5分) → 答え合わせ

③ 問題集 P.19, 20 暗号化を解く (15分)

(問6 チヒロは・・・飛ばす)

☆早く終わってしまった人はタイピング

④ 答え合わせ・解説 (10分)

次の暗号を解いてみよう

3

Ucjj Zcgle

正解は・・・

Well being

昔の暗号は？

4

シーザー暗号

非常に簡単な換字法の1つ
アルファベットの文字を一定の文字数分だけずらす

転置法

平文の文字を一定の規則で並べかえる方式

E N C R Y P T I O N

↓ 1字ずらす

F O D S Z Q U J P O

「暗号化」を意味する「ENCRYPTION」のそれぞれのアルファベットを1字分ずらすと、「FODSZQUJPO」と暗号化される。

E N C R Y

↓ ↗ ↓ ↗ ↓ ↗ ↓ ↗ ↓

P T I O N

「ENCRYPTION」を2つに分けて、上のように並べ、縦に文字を拾っていくと、「EPNTCIROYN」と暗号化される。

図28 換字法（シーザー暗号）の例

①暗号化

データの内容を第三者にわからなくする技術または手法

こんにちは

暗号化

gejg23ga2g

②平文(ひらぶん)

暗号化されていないデータのこと



③復号

暗号化されたデータをもとのデータに復元すること。

gejg23ga2g

復号

こんにちは



🔑 共通鍵暗号方式

6

暗号化と復号に使う鍵が同じ方式

平文

こんにちは。お久しぶり
です。お元気ですか？

暗号化後

Gapaw3r2023`*#(“fwdk#
” *~” ff4ikuy#!” `>MVE



さくら



ゆうじーん

🔑 共通鍵暗号方式

7

暗号化と復号に使う鍵が同じ方式



さくら



こんにちは。お久しぶりです。お元気ですか？



ゆうじーん







共通鍵暗号方式 必要な鍵の数は？

8

- 暗号化、復号に同じ鍵を用いるため2人でやりとりする時は1本でやりとりできる。
- 3人の場合はお互いに1本ずつ必要なので3本



人数	2人	3人	4人	5人
鍵数	 1	 3	 6	 10



- 上のような図を書くか $n(n-1)/2$ で求めることができる



公開鍵暗号方式

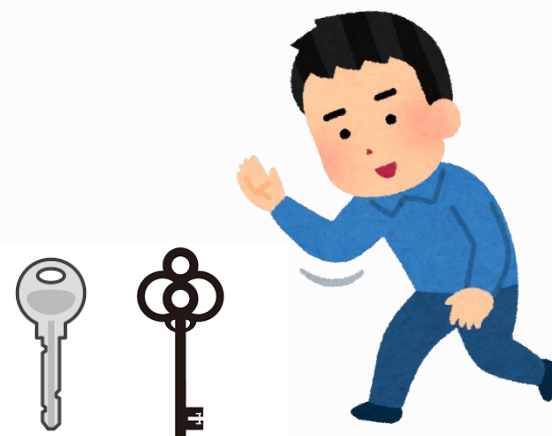
9

暗号化と復号に使う鍵が異なる方式
鍵ペア → 秘密鍵  公開鍵 

- ① 受信者が秘密鍵と公開鍵を作成
- ② 送信者は受信者より公開鍵を得る
- ③ 送信者は公開鍵で平文を暗号化
- ④ 受信者は自分の秘密鍵で復号



さくら



ゆうじーん



公開鍵暗号方式

10

暗号化と復号に使う鍵が異なる方式
鍵ペア → 秘密鍵



公開鍵



さくら



ゆうじーん

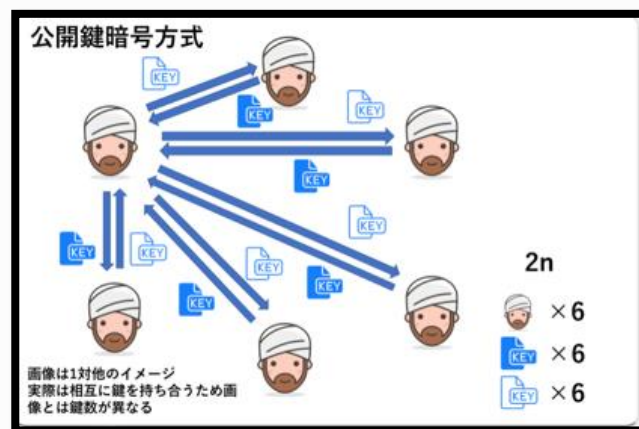
- ① 受信者が秘密鍵と公開鍵を作成
- ② 送信者は受信者より公開鍵を得る
- ③ 送信者は公開鍵で平文を暗号化
- ④ 受信者は自分の秘密鍵で復号



公開鍵鍵暗号方式 必要な鍵の数は？

11

- 暗号化、復号に違う鍵を用いるため2人でやりとりする時は**2本必要**。
- 3人の場合はお互いに2本ずつ必要なので6本必要



- 図を書くよりは $2n$ で求めるほうが早い

共通鍵暗号方式と公開鍵暗号方式の違い

12

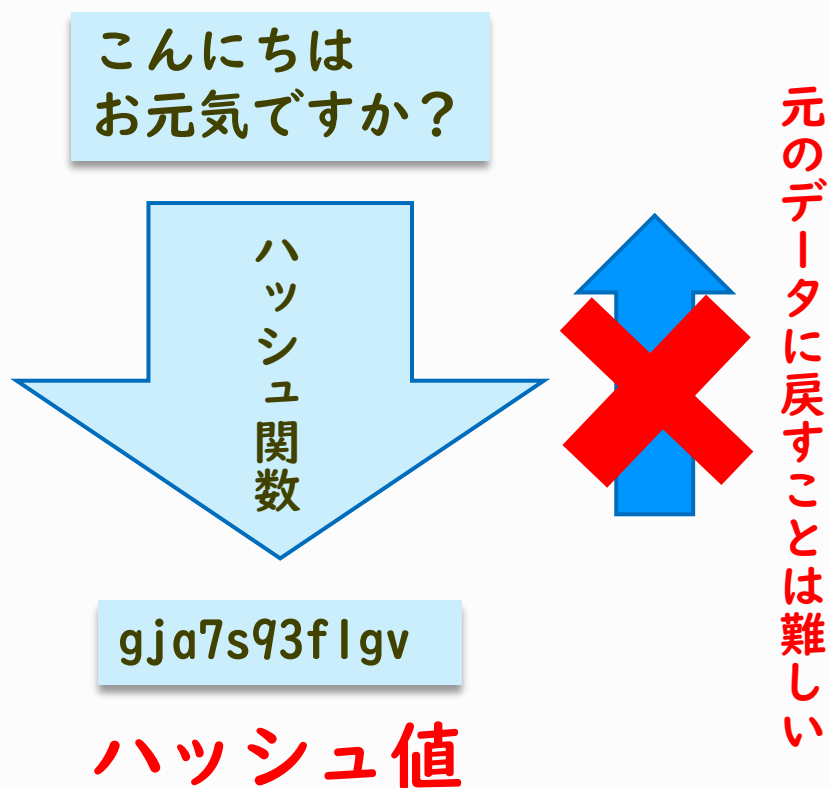
	共通鍵暗号方式	公開鍵暗号方式
メリット	公開鍵暗号方式に比べて暗号化と復合が (① 速い (高速))	(② 公開鍵の方は公開情報なので漏洩しても問題がない)
デメリット	人数分の異なる共通鍵を準備し、これを安全に共有し使い分ける必要があるので、鍵の管理が大変	共通鍵暗号方式に比べて暗号化と復号に (③ 時間がかかる)

ハッシュ値について

13

ハッシュ値の特徴

- 入力値が同じ内容なら、必ず同じハッシュ値となる
- 入力文字を少しでも変えると全く違うハッシュ値となる



公開鍵暗号方式とハッシュ値の技術を応用することで、「誰が送信したのか」と「途中で改ざんされていないか」を確認できるようにした

⇒①デジタル署名（電子署名）

デジタル署名流れ

15



さくら

ゆうじんの
の公開鍵



こんにちは
お元気ですか？

ハッシュ
関数

gja7s93flgv

自分の秘密鍵
で暗号化



ゆうじん

ゆうじんの
秘密鍵

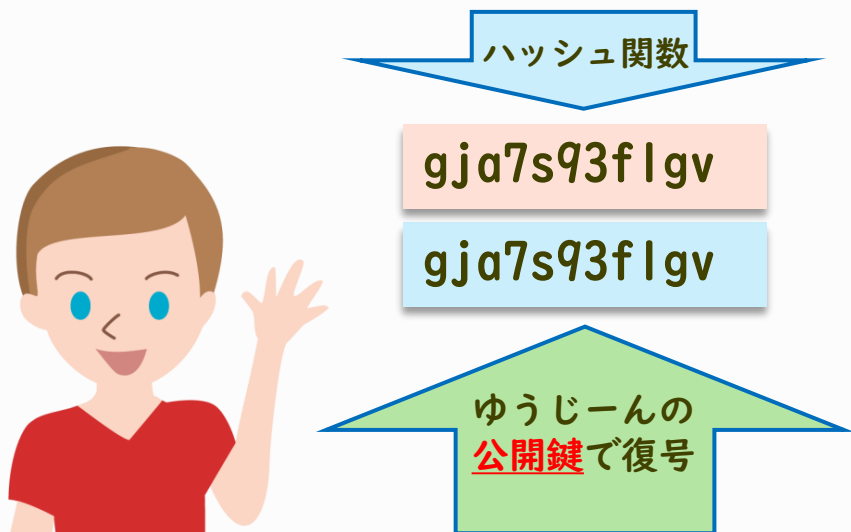


デジタル署名

ハッシュ値を秘密鍵で暗号化したもの

デジタル署名流れ

16



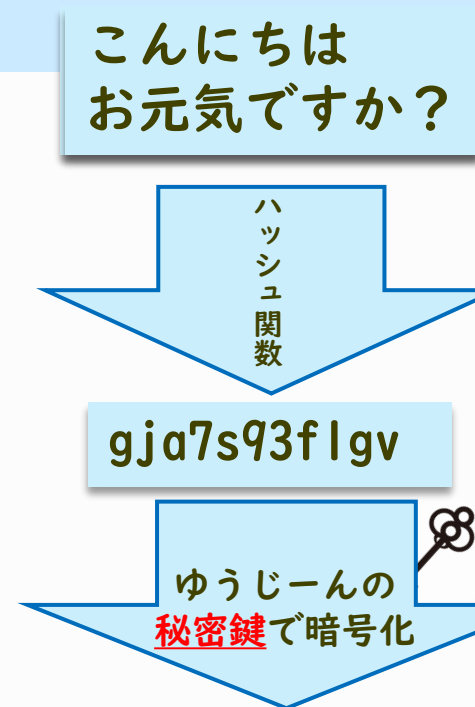
さくら

ゆうじんの
公開鍵



一致した！！
(改ざんされていない)
⇒完全性確認

復号できた！！
⇒真正性確認



ゆうじん

ゆうじんの
秘密鍵



デジタル署名

ハッシュ値を秘密鍵で暗号化したもの

デジタル証明書

17

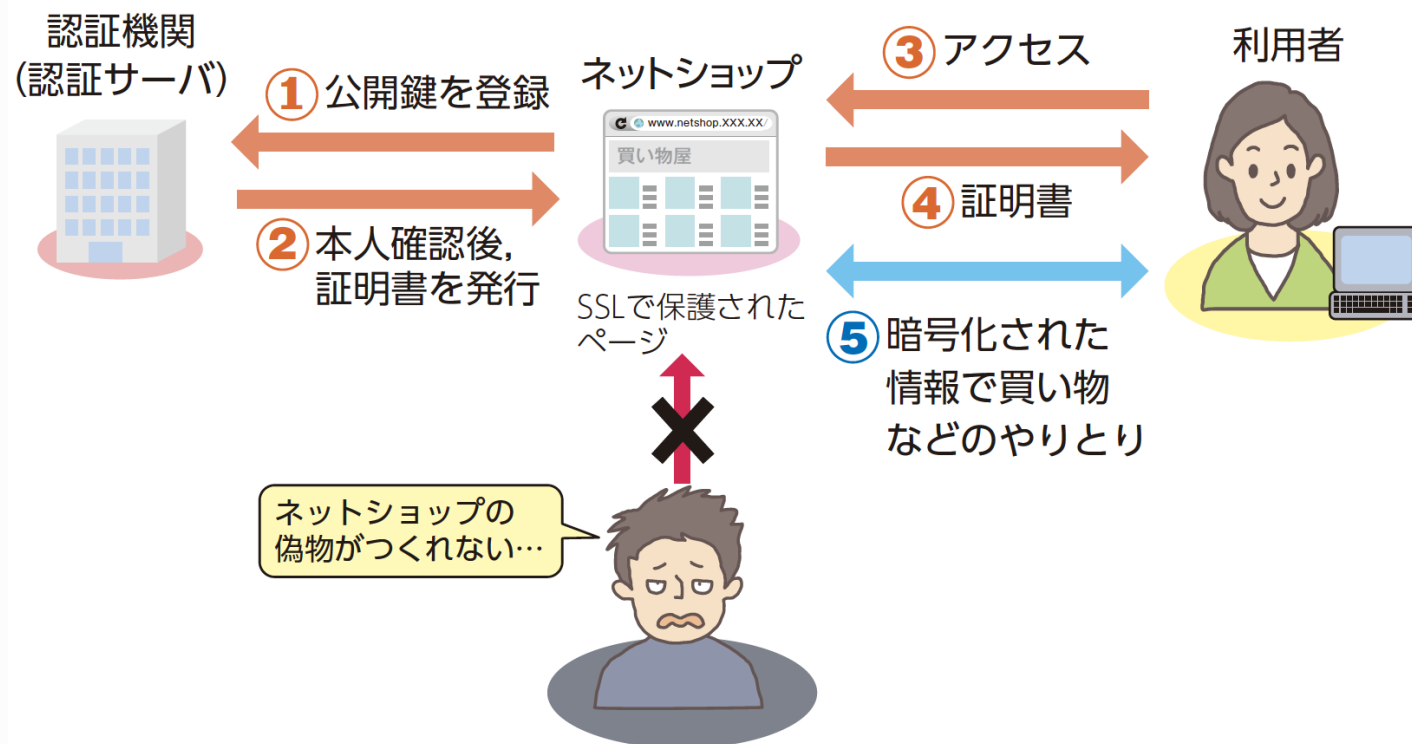
- 公開鍵（デジタル署名）が確かに本人のものであることを、

認証機関（認証サーバ）とよばれる信用できる第三者が証明するしくみがある

- デジタル署名を使いたい人は、認証機関に登録して、

③デジタル証明書

（電子証明書）の発行を受ける



①SSL

インターネット上で情報を暗号化して送受信する手順の決まり

- SSLを使用していないウェブページのURLは「http://」ではじまるが、SSLを利用したページは「http**s**://」となる
- 近年後継である（②TLS）に置き換わってきているため（③SSL/TLS）と表記されることが多い

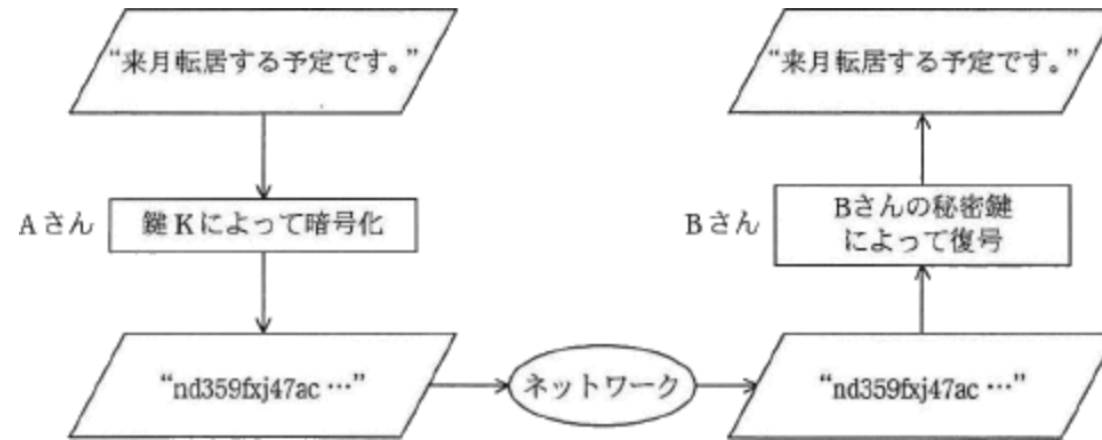


図34 SSLとデジタル証明書

問 2 基本情報技術者試験問題

19

公開鍵暗号方式を用いて、図のようにAさんからBさんへ、他人に秘密にしておきたい文章を送るとき、暗号化に用いる鍵Kとして、適切なものはどれか。



ア Aさんの公開鍵

イ Aさんの秘密鍵

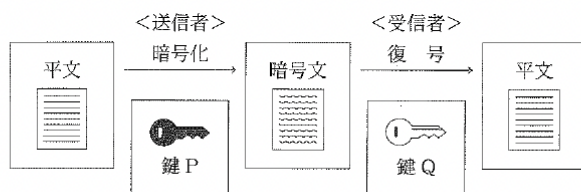
ウ Bさんの公開鍵

エ 共通の秘密鍵

・考え方は問1と同じ。

公開鍵暗号方式では受信者の公開鍵で暗号化を行い、受信者の秘密鍵で復号する

問 3 次の図は、下線部(c)に関連して先生が生徒たちに見せた公開鍵暗号方式における暗号化と復号の過程に関する模式図である。模式図を説明した文中の空欄 工 ~ 力 に入れるのに最も適当なものを、後の解答群のうちから一つずつ選べ。



暗号化と復号の過程は、工 → オ → 力 の順で行われる。

図 公開鍵暗号方式における暗号化と復号の過程の模式図とその説明

工 ~ 力 の解答群

- ① 送信者が公開鍵 P と秘密鍵 Q のペアを作成して鍵 P を公開し、受信者が鍵 P を入手する。
- ② 送信者が秘密鍵 P と公開鍵 Q のペアを作成して鍵 P を公開し、受信者が鍵 P を入手する。
- ③ 送信者が秘密鍵 P と公開鍵 Q のペアを作成して鍵 P を公開し、送信者が鍵 P を入手する。
- ④ 送信者が平文を公開鍵 P で暗号化する。
- ⑤ 送信者が平文を秘密鍵 P で暗号化する。
- ⑥ 受信者が公開鍵 Q で暗号文を復号する。
- ⑦ 受信者が秘密鍵 Q で暗号文を復号する。

公開鍵暗号方式は

- ① **受信者**が公開鍵と秘密鍵を作成
- ② その後**送信者**に**公開鍵**を渡す
- ③ 送信者は**公開鍵**を使い暗号化
- ④ 受信者は**秘密鍵**で復号

答え 工 ①

答え オ ④

答え 力 ⑦

HTTPSの通信にはSSLが使われていた。

最近は後継のTLSが登場してSSL/TLSと表記されHTTPSの通信に使用されている。

・デジタル署名でわかるのは、「誰が送信したものか」と
「途中で改ざんされていないか」

a 次の文章中の空欄 に入れるのに最も適切なものを、後の①～④のうちから一つ選べ。

インターネットで情報をやり取りする際、発信者が本人であることを確認するためにデジタル署名が利用できる。また、デジタル署名を用いると、その情報が を確認できる。

- ① 複製されていないか
- ② 暗号化されているか
- ③ 改ざんされていないか
- ④ どのような経路で届いたか
- ⑤ 盗聴されていないか

答え ②

問Ⅰ シーザ暗号【ア、イ、ウ、エ】

23




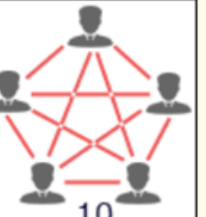
- ア アルファベット「DQCX」を3文字ずらすと「ANZU」
- イ アルファベットは全部で26文字。自分自身を含めない
ので答えは25通り
- ウ 1～5文字だと5通り。さらに一文字ずつずらす
方法が5通りなので5！（5の階乗）で120通り
- エ 表から読みとり「かのう」

問3 共通鍵暗号方式【オ、カ】

24

- 共通鍵暗号方式は1対1のやりとりでは鍵が1つ必要（図参照）



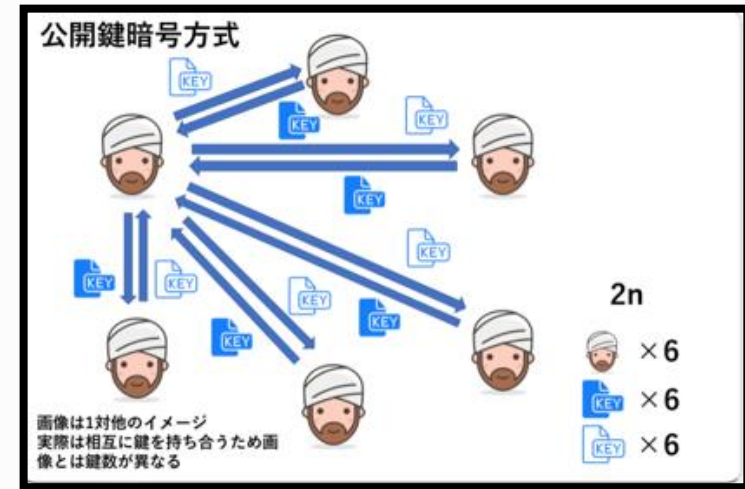
人数	2人	3人	4人	5人
鍵数	 1	 3	 6	 10

- オ 4人（Aさん、Bさん、Cさん）だとAとBのやり取りに1つ、AとCのやり取りに1つ、BとCのやり取りに1つの合計6個必要と考える
- カ 鍵の数を求める式は $n(n-1/2)$ で求めることができるので、10人の場合は45個必要

問3 公開鍵暗号方式【ケ、キ、ク】

25

- 公開鍵暗号方式は1対1でやり取りする場合
公開鍵と秘密鍵の2つが必要である

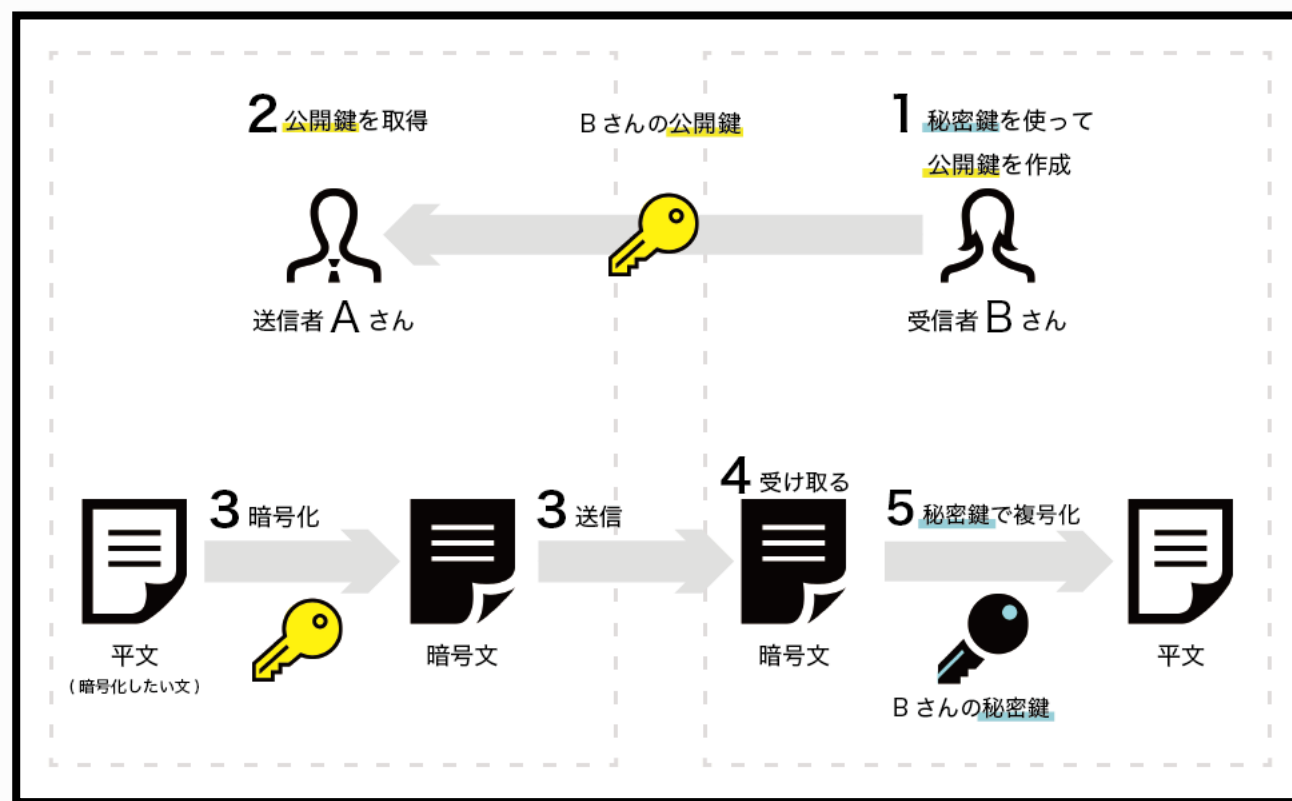


ケ 3人の場合は3人×2つの鍵=6個必要である
キ、ク 鍵の数を求める式は $2n$ なので、4人の場合は8個、
10人の場合は20個必要である。

問4 公開鍵暗号方式【い・ろ】

26

い・ろ 公開鍵暗号方式では受信者の公開鍵で暗号化を行い、
受信者の秘密鍵で復号する



問5 公開鍵暗号方式と共通鍵暗号方式【サ】

27

プリントの表を参考に解いていく。

	共通鍵暗号方式	公開鍵暗号方式
メリット	鍵が1つなので公開鍵暗号方式に比べて暗号化と復号が (① 簡単にできる)	(②公開鍵は公開情報なので漏れても問題ない)
デメリット	人数分の異なる共通鍵を準備し、これを安全に共有し使い分ける必要がある ので、鍵の管理が大変	共通鍵暗号方式に比べて鍵が2つあり 処理が複雑なため暗号化と復号に (③ 時間がかかる)

- ① 鍵が1つなので処理が複雑でなく、処理速度が速い
- ② 鍵が2つなので処理が複雑で、処理速度が遅い
- ③ 公開鍵は公開情報なので漏れても問題ない

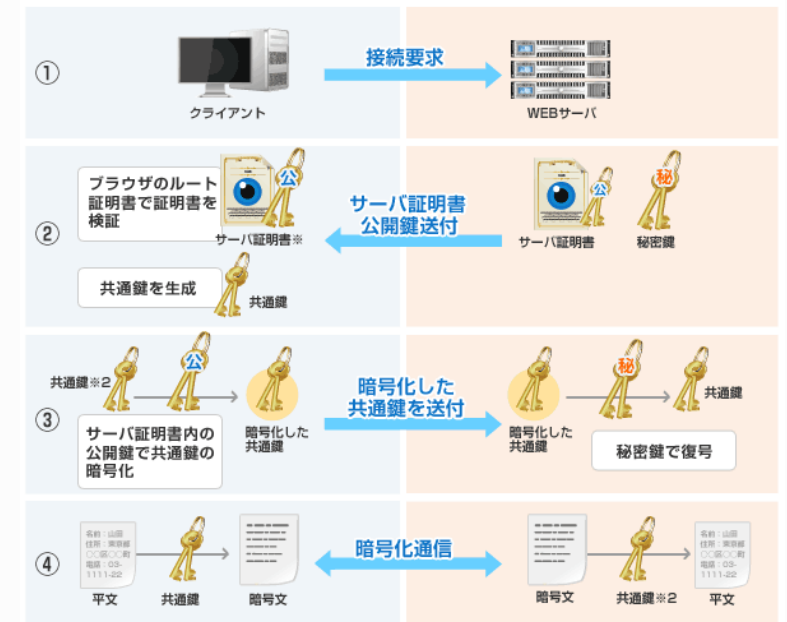
答え ②

問6 SSL/TLS【シ】

28

・プリントよりSSL/TLSの流れは

- ①利用者がweb サーバに接続を要求
- ②利用者に公開鍵と電子証明書（サーバー証明書）を送付
- ③利用者はデータを暗号化するために共通鍵を作成
- ④暗号化した共通鍵を送付する
- ⑤受信者は秘密鍵で復号する

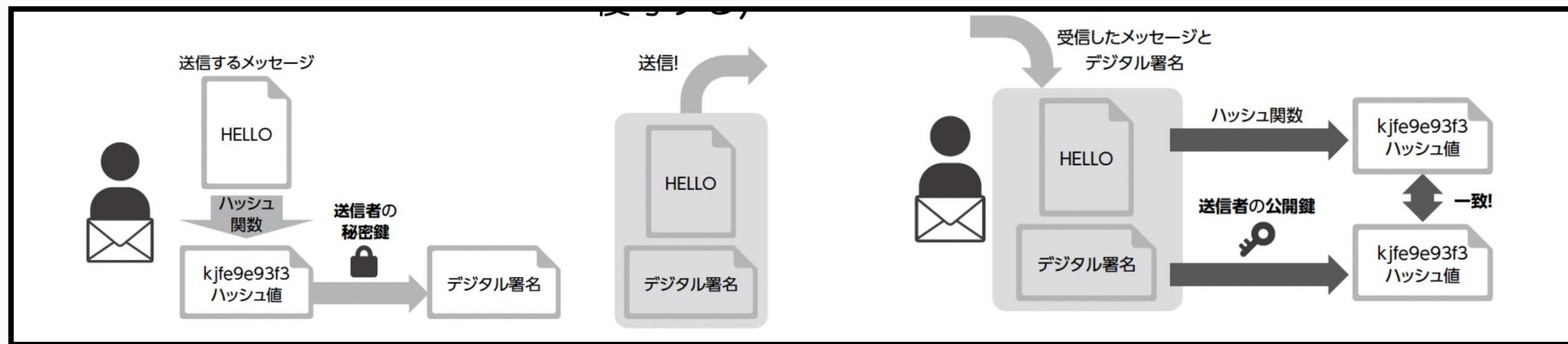


答え ②

問7 デジタル署名【セ】

29

- デジタル署名は公開鍵暗号方式と違い
送信者の秘密鍵で暗号化し、送信者の公開鍵で復号する
(公開鍵暗号方式は受信者の公開鍵で暗号化し、
受信者の秘密鍵で復号)



答え 0

問8 デジタル署名の説明【セ】

30

- ・デジタル署名でできることは
「送信したデータが本人のものであること」と
「文章が改ざんされていないか」がわかる
- ① 改ざんされていないかはわかるが修正はできない
- ② 改ざんされていないかはわかるが、改ざん場所の特定はできない
- ③ 送信されたデータが本人のものであるかは特定できるがそれ以外の誰のものであるかは特定できない

答え ①

問9 デジタル署名の説明【ソ】

31

- ①シーザー暗号などは自力で解くことができるため、なりすましを防ぐ効果がない。暗号はなりすましを防ぐために作られた技術ではない
- ②人間の発明力を示すのに暗号が作られたわけではない
- ③情報の隠蔽を防ぐ効果はなく、
そのためにも作られていない

答え 0