暗号化とデジタル署名について理解しよう♪

［１学期授業用プリント No.３］
問題集　P.19,20【暗号化】

３年（　　）組（　　）番　名前（　　）

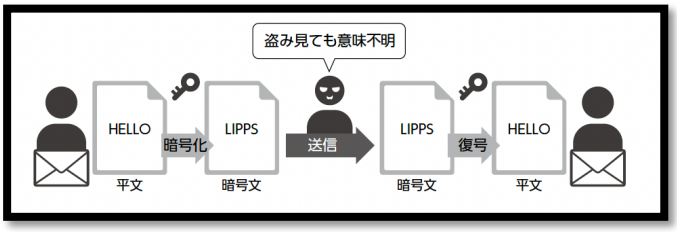
1　データをやり取りするときに誰かに盗聴されたり、中身を知られてしまうと大変です。
そこで重要になってくるのが暗号です。

（①暗号化）・・・暗号にすること。暗号化された文を暗号文という。

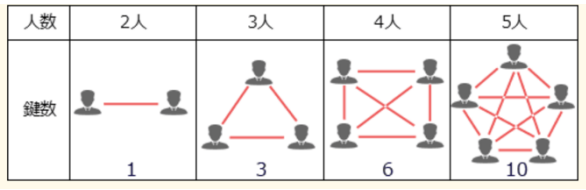
（②平文）・・・暗号化されていない情報。暗号文を平文に戻すことを（③ 復号　　）という。

2　ではどのような暗号方式があるのか知ろう。

（①　共通鍵暗号方式　）・・・暗号化と複合で同じ鍵を（共通鍵）を用いる方式。



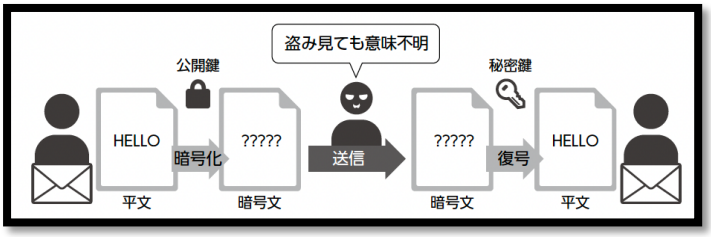
すべての鍵を秘密にしなければならない。
→送り手ごとに別の鍵が必要というデメリットがある。

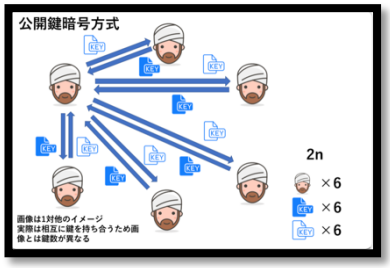


☆必要な鍵の数の計算は（②n(n−1)／2）で求めることができる。

（③公開鍵暗号方式　）・・・暗号化と複合に別々の鍵を使う方式。
→受信者の公開鍵と秘密鍵を使う。

流れ　①受信者が公開鍵と秘密鍵を作る。　②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受信者は秘密鍵を使い復号





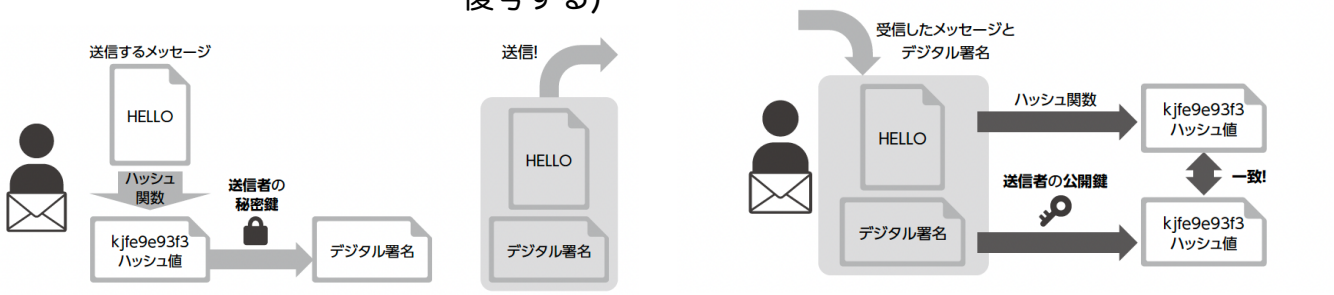
☆必要な鍵の数の計算は（④2n）で求めることができる。

3　共通鍵暗号方式と公開鍵暗号方式のメリット、デメリットをまとめよう。

	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　）

4　デジタル署名について知ろう。

（①　デジタル署名　　）・・・公開鍵暗号やハッシュ値を利用したもので本人が署名したこと、文章の内容が改ざんされていないことを確認できる。
ポイントは(②送信者の秘密鍵で暗号化して、送信者の公開鍵で復号する)



（③　デジタル証明書（電子証明書）　）・・・①を認証機関に登録し、
本人のものであると証明できるもの

●デジタル署名の流れ　①送信者が公開鍵と秘密鍵を作成 ②送信者が受信者に公開鍵を渡す ③送信者は秘密鍵を使いハッシュ値を暗号化 ④受信者は公開鍵を使い復号 ⑤復号されたハッシュ値と送信者が作ったハッシュ値を比較

5　みんなが使うインターネットではどのような暗号技術が使われているか知ろう。

（①　SSL　）・・・データを暗号化して送受信する仕組み
☆近年後継である（② TLS　　）に置き換わってきている。
↓
（③ SSL/TLS　）と表記されることが多い

③を利用した web ページの特徴は？

→ http:のところが https:となっている

5　暗号の歴史について

(１)次の暗号を解いてみよう。

Ucjj Zcgle →

（2）（1）のようにアルファベットをずらして暗号を作る方法を（①　　）という。

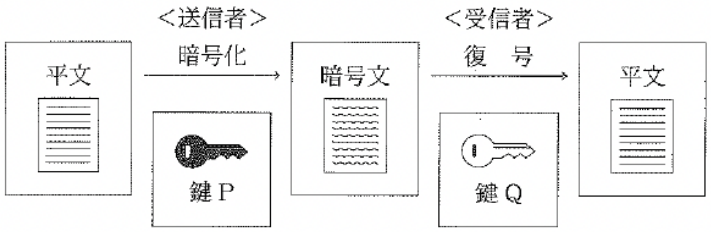
基本情報技術者試験　問1

Xさんは，Yさんにインターネットを使って電子メールを送ろうとしている。電子メールの内容を秘密にする必要があるので，公開鍵暗号方式を使って暗号化して送信したい。電子メールの内容を暗号化するのに使用する鍵はどれか。

ア　Xさんの公開鍵
イ　Xさんの秘密鍵
ウ　Yさんの公開鍵
エ　Yさんの秘密鍵

全統模試_2025 年度

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 エ ～ カ 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，エ → オ → カ 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

エ ～ カ の解答群

⓪　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。
①　受信者が公開鍵 P と秘密鍵 Q のペアを作成して鍵 P を公開し，送信者が鍵 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　受信者が秘密鍵 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。

c　インターネットを介して安全な通信を行うための暗号化技術として，SSL や TLS と呼ばれるものがある。SSL や TLS に関する記述として**誤りを含むもの**を，次の⓪～③のうちから一つ選べ。 ウ

⓪　SSL や TLS はデータを暗号化した上で通信する技術であり，SSL や TLS を使っても，通信先が安全な相手であることは保証されない。

①　SSL や TLS を使わない通信では，通信しているデータを第三者に傍受された場合，解読されやすい。

②　HTTP を用いた通信では，SSL や TLS は使われていない。

③　HTTPS を用いた通信では SSL のみが使われており，TLS は使われていない。

デジタル署名　2025 年度共通テスト

a　次の文章中の空欄 ア に入れるのに最も適当なものを，後の⓪～④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 ア を確認できる。

⓪　複製されていないか

①　暗号化されているか

②　改ざんされていないか

③　どのような経路で届いたか

④　盗聴されていないか