# txt030421 暗号化技術

## ①　暗号化

### ⓐ　暗号化とは

暗号化は文章に対して変換を施し、第三者には何が書かれているか分からない状態にすることである。変換する前の文を平文(ひらぶん)、変換された状態の文書を暗号文という。暗号にはコードとサイファーがある。

コードはあるまとまりのある語や句を他のもので置き換えることである。当事者同士が理解でき、第三者に理解できないものならば何でもよい。サイファーは通信文の文字を１対１に置き換えるものである。暗号というとサイファーだけを指す場合が多い。

### ⓑ　古代の暗号化

暗号は古来より主に軍事目的に利用されており、基本的なアイデアは、古代ギリシャ・ローマ時代からすでに存在していた。ギリシャ時代にはスキュタレーと呼ばれる指揮棒に文書を巻き付けて、文章内の文字の位置を置き換える方式の暗号化が用いられた。

シーザ暗号は文字を何文字かずらしたものに置き換える方式である。ＡをＣ、ＢをＤに置き換えることで、ＡＢＣをＣＤＥと表す。文書内の文字の位置を置き換える置換や他の文字との置き換えである換字というアルゴリズムは現代においても暗号を構成する基本要素になっている。

これらの暗号はアルゴリズムおよび暗号化・復号の鍵は、共に秘密にしておく必要があった。

### ⓒ　20世紀の暗号化

1977年にアメリカ合衆国商務省標準局によって、商業用の標準暗号ＤＥＳが制定された。このとき、暗号アルゴリズムが仕様として公開され、暗号アルゴリズムは必ずしも秘匿されるものではなくなった。アルゴリズムが公開されていても、解読不可能な強度を持つことが暗号アルゴリズムに対して要求されるようになった。鍵を秘密にしておく暗号化方式を、秘密鍵暗号、または共通鍵暗号と呼ぶ。

1976年に公開鍵暗号の概念が発表された。暗号アルゴリズム、鍵の一部を公開しても解読は不可能という画期的な概念である。この方式を公開鍵暗号方式という。1978年に大きな数の素因数分解の困難性に基づいたＲＳＡ方式が発表され、1982年に離散対数問題の困難性に基づいたＥＬＧamal暗号が考案され、1985年に楕円曲線上の離散対数問題の困難性に基づいた楕円曲線暗号が考案されている。公開鍵暗号方式の出現によって、古典暗号では第三者に対する情報の秘匿に限られていた暗号の利用目的は、相手認証、メッセージ認証という認証機能を持ち合わせるようになり、大きく広がった。

## ② インターネットの脅威

### ⓐ 盗聴

盗聴は、通信内容を第三者に知られたり、盗まれたりしてしまうことである。通信内容が第三者に漏れてしまう危険性があると、社外秘の文書やプライベートな情報などを安心して通信できなくなる。

### ⓑ 改ざん

改ざんは、通信内容を書き換えられてしまうことである。送信者から受信者に送ったデータを第三者が途中で横取りし、内容を一部変更して受信者に向けて送り出すことである。契約書をやり取りする途中で契約金額を書き換えられるようなことが起こるネットワークでは、安心してビジネスに利用できなくなる。

### ⓒ なりすまし

なりすましは、通信の相手に正体を偽ることである。対面して話を行うときには相手が本人であることを確認できるが、ネットワークでは不可能である。通信相手が本人であることを確認できなければ、インターネットをビジネスに使用できなくなる。

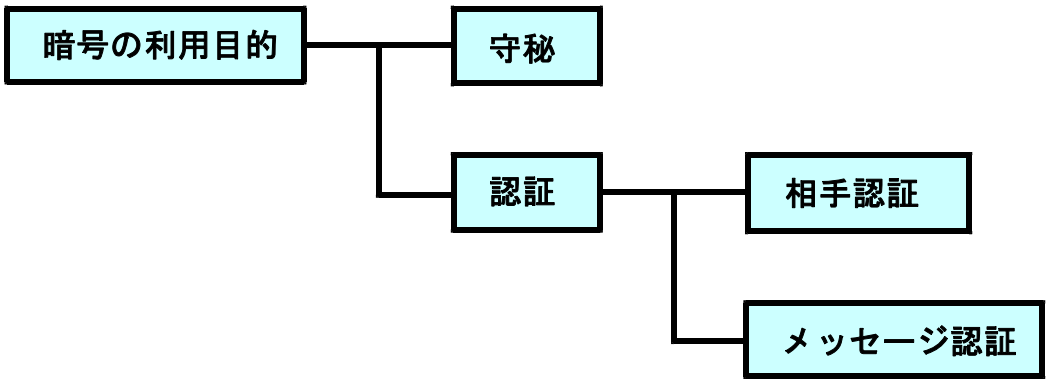
### ⓓ 否認

否認は、通信した事実やその内容を否定することである。イクターネットを通じて契約した事実や契約した内容がその後に否定されたり、修正されると、インターネットを使用して契約行為をすることができなくなる。

## ③ 暗号化の利用目的

### ⓐ 暗号化の目的

守秘、認証、アクセス管理の３つの目的がある。



## ⓑ　守秘

二者間での情報秘密の共有、第三者に対する情報秘匿、第三者の傍受・盗聴に対する安全性確保をはかるものである。

## ⓒ　認証

㋐　相手認証

相手認証は本人確認ともいわれ、相手が確かに本当の相手であることを確認する手段である。単純な方式ではパスワードを使用する。第三者のなりすましに対する対策である。

㋑　メッセージ認証

メッセージ認証はデータの完全性と否認防止がある。データの完全性は通信途上で内容が改ざんされていないことを検査し、保証する手段であり、第三者の不正に対する対策である。否認防止は、送信側は送ったことを否定できないことの保証であり、受信側は受け取ったことを否定できないことの保証である。「言った／言わない」ということを避けるための手段で、当事者の不正に対する対策である。

## ⓓ　アクセス管理

アクセス管理は正当な利用者のみアクセスでき、不正なアクセスができないことである。

# ④　暗号の原理

## ⓐ　換字暗号と転置暗号

暗号化で文字をずらせる換字暗号や文字の順序を変える転置暗号が基本的な暗号変換であり、ずらせる文字数などが鍵となる。非常に長い乱数鍵との排他的論理和で暗号化／復号するバーナム暗号もある。

| | | | |
|---|---|---|---|
| 元データ | １００１０１１１１０００１０１ | | |
| 元データ | １００１０１１１ | １１０００１０１ | 転置処理 |
| 転置後データ | ０１１１１００１ | ０１０１１１００ | |
| 元データ | ０１１１１００１ | ０１０１１１００ | 換字処理 |
| 暗号鍵 | １１００１００１ | １１００１００１ | |
| 暗号データ | １００１０００１ | １００１０１０１ | |

## ⓑ　ＸＯＲ演算

ＸＯＲ演算は、排他的論理和の演算であり、２つの入力のどちらか片方が真でもう片方が偽の時には結果が真となり、両方とも真あるいは両方とも偽の時は偽となる論理演算である。こ

の考え方は、次のストリーム暗号やパーナム暗号、換字処理に活用されている。

## ⓒ　ストリーム暗号

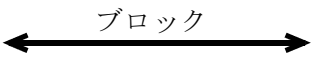
共通鍵暗号はストリーム暗号とブロック暗号の２種類に分類される。ストリーム暗号は、ブロックに区切らず１ビット単位あるいは１バイト単位で逐次暗号化する方式である。任意長の鍵ストリーム列を生成させ、これと入力の平文を演算させる方式である。１ビットや１バイト単位でデータを暗号化できるので、ＳＳＬや無線ＬＡＮなど、ネットワークのトラフィックを暗号化するために利用されている。

暗号化したデータを伝送する場合、ブロック暗号ではブロック全体が揃わないと復号できないが、ストリーム暗号は受信したデータを即座に復号化できる。ブロック暗号がデータ量をブロック長の整数倍に調整するのに対し、ストリーム暗号は平文の量と暗号化後のデータ量が常に一致するという特性がある。応答性が重視される通信用途で用いられることが多い。

## ⓓ　ブロック暗号

ブロック暗号は与えられたデータ(平文)を６４ビットや１２８ビットなどあらかじめ定められた固定長のブロックに区切り、この単位ごとに暗号化していく方式である。ブロックごとに分割された平文を内部でさらに分割、転置し、暗号鍵との加算を繰り返していくことで、暗号化を行う。鍵の長さ(鍵長)が大きいほど複雑な暗号を作成できる。ブロック長及び鍵長は固定長のものと、可変長のものがあるが、処理のし易さから固定長のものを採用したものが多い。復号もブロック単位に処理される。

軍事用途で使われることが多かったストリーム暗号に比べて、ブロック暗号は企業など民間で開発されたものが多く、さまざまな種類のものが存在する。代表的なブロック暗号としては米国政府の標準として採用されているＤＥＳ、ＤＥＳを３回かけてさらに安全性を向上させたTriple-ＤＥＳ、ＳＳＬなどＷｅｂの暗号化に利用されているＲＣ５、メール用の暗号PGPで採用されているＩＤＥＡ、ＤＥＳの次世代版として期待されているＡＥＳなどがある。




| | | |
|---|---|---|
| 元データ | 10001001001001110110100101100101 | 元データと鍵との排他的論理和 |
| 暗号化鍵 | 11011010010100111101101001010011 | |
| 暗号データ | 01010011011101001011001100110110 | 演算結果 |

## ⓔ　一方向性関数

一方向性関数は、計算すること自体は比較的容易だが、計算結果から元の情報を逆算することは極めて困難であるような関数のことである。数学的に記述すると、関数ｆが任意のｘについてｙ＝ｆ(ｘ)の計算は簡単であるが、ｙ＝ｆ(ｘ)となるｙが与えられたとき、ｆの逆関数ｇを用いてｘ＝ｇ(ｙ)を導き出すのは事実上不可能である場合に、関数ｆは一方向性関数と呼ばれる。一方向性関数は、暗号理論などで用いられる概念でり、素因数分解問題の困難性を用いたものが代表的名ものである。一方向性関数を利用した暗号は、相手に暗号化鍵を教える際に、

他人に漏れても直ちに暗号を解読されるという事態にならないという考えに基づいている。

この考え方は公開鍵暗号方式に利用され、ハッシュ関数として活用されている。

### ⓕ　ハッシュ関数

ハッシュ関数は、長い文章やデータを固定長のビット列に圧縮する一方向性の関数で、圧縮された値をハッシュ値と呼ぶ。ハッシュ関数は一方向性のため、ハッシュ値から元のデータを復元することはできない。従って、ハッシュ値にディジタル署名を付して、本人性と文書の真正性の証明に利用したり、証拠の保全・開示に広く利用される。

### ⓖ　デジタルフォレックス

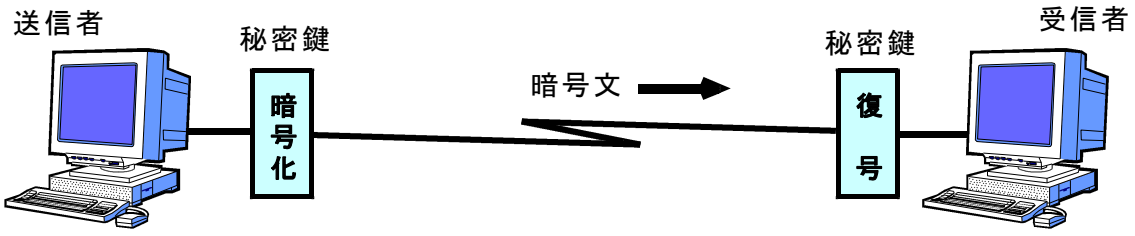
デジタルフォレンジックは、犯罪捜査や法的紛争などで、電子機器に残る記録を収集・分析し、その法的な証拠性を明らかにする手段や技術のことである。対象となるのはパソコンやサーバ、ネットワーク機器、携帯電話、情報家電など、デジタルデータを扱う機器全般である。

関係先の機器を押収して記憶装置から事件の証拠となるデータを抽出したり、サーバや通信機器などに蓄積された通信記録から違法行為の証拠となる活動記録を割り出したり、破壊・消去された記憶装置を復元して証拠となるデータを割り出したりといった技術、コピーや消去、改ざんが容易であるというデジタルデータの性質に対応して、データが捏造されたものかどうかを検証する技術、記録の段階でデータが改ざんできないよう工夫したり、ハッシュ値やデジタル署名などで同一性を保全する技術などの活動が該当する。

デジタルフォレンジックは、不正アクセスや機密情報漏洩など、コンピュータや通信ネットワークに直接関係する犯罪における捜査手法として注目されたが、社会へのＩＴの普及・浸透に伴って、一般の刑事事件などでも捜査や立証に活用されるようになってきている。

## ⑤　秘密鍵方式

### ⓐ　秘密鍵方式とは




秘密鍵方式は送信元の暗号化と受信先の復号を同じ共通鍵で行う方式で、送信者と受信者が共に共通鍵を秘密にもっている暗号化方式である。アルゴリズムは公開されている。代表的なものに米国の標準化暗号方式のＤＥＳがあったが、技術進歩により安全性が低下したため、新たな共通鍵ブロック暗号を世界から公募した結果、ベルギーの研究者が設計したラインダールがＡＥＳとして採用された。ＡＥＳはブロック暗号で、ブロック長は１２８ビット、鍵長は１

２８ビット、１９２ビット、２５６ビットの３つが利用できる方式である。

### ◇ＤＥＳ暗号

ＤＥＳ暗号は、暗号化と復号に同じ暗号鍵を用いる共通鍵暗号（秘密鍵暗号）の一つで、データを６４ビット単位に区切って処理するブロック暗号である。鍵長は５６ビットだが、パリティチェック用の８ビットを加えた６４ビットを鍵データとして管理する。

ＤＥＳでは変換処理を行った結果に再度同じ処理を行うという繰り返し（ラウンド）を１６回行うが、それぞれのラウンドでは元の鍵から一定の計算により生成した異なる鍵データを用いる。最初にデータを３２ビットずつ半分（Ｌ，Ｒ）に分割し、一回のラウンドでは半分（Ｒ）を変換して残りの半分（Ｌ）と合成する処理を行う。次のラウンドでは前回の合成結果を新たなＲ、変換に用いた半分（Ｒ）を新たなＬとして同じ処理を行う。このような処理方式はファイステル構造と呼ばれ、暗号化と復号が同じアルゴリズムになる（適用する鍵データを変えるだけでよい）ことからＤＥＳ以外にも様々な暗号方式に広まった。

### ◇ＡＥＳ暗号

ＡＥＳ暗号は、ＤＥＳの後継として米国の国立標準技術研究所によって制定された新しい暗号化規格である。ＤＥＳの後継となる共通鍵方式の暗号化規格が公募された時、世界中から21の方式が提案された。それらの暗号方式の中から、暗号強度や安全性、ハードウエアやソフトウエアでの実装のしやすさや性能（速度）、計算に必要なハードウエアリソースや必要な電力、鍵長やブロック長などに対する柔軟性、知的財産的な評価など、さまざまな視点から評価・検討された。最終的にラインダール暗号化方式が選ばれた。ラインダールは鍵長やブロック長が可変の共通鍵方式のブロック暗号である。提案されたラインダーではいくつかの鍵長やブロック長が選べたが、最終的には、鍵長１２８、１９２、２５６ビット、ブロック長１２８ビットのパラメーターだけを使うことになり、これが正式なＡＥＳ規格となった。

ＡＥＳには鍵長に応じてＡＥＳ１２８、ＡＥＳ１９２、ＡＥＳ２５６の３種類のバリエーションがある。鍵長を長くすれば、それだけ安全性が増すと考えられるが、その分計算量が増えるのでどれを使うかはケースバイケースである。現在の所は、ＡＥＳ１２８で十分と考えられている。

## ⑥　公開鍵方式

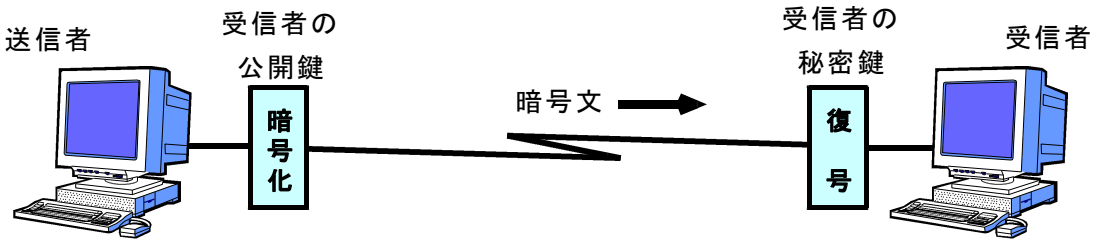
### ⓐ　公開鍵方式とは

公開鍵暗号方式は通信文を送信する場合、送信元で公開鍵により暗号化し、受信先で専用の秘密鍵で復号する方式である。暗号化する鍵と復号する鍵が異なり、片方の鍵を公開し、もう一方の鍵は秘密にした暗号化方式である。代表的なものにＲＳＡ方式がある。

公開鍵から秘密鍵を発見することは不可能であり、公開鍵を管理する必要がない。秘密鍵は自分だけが持てばよいので、鍵管理が簡単で安全度が高い。論理が複雑なため処理時間が長くなり、処理速度は共通鍵方式よりも遅い。公開鍵暗号を守秘に使う場合、送信者は受信者の公

開鍵を用いて暗号化し、暗号文を送る。受信者は自分だけが知っている秘密鍵を用いて復号し、元の平文を得ることができる。

鍵の配布やデジタル署名に利用される。




## ⓑ　ＩＦ型、ＤＬ型、ＥＣ型

公開鍵暗号は、ＩＦ型、ＤＬ型、ＥＣ型に分類できる。ＩＦ型は、素因数分解の困難性に基づくものである。ＤＬ型は、素数の剰余類群における離散対数問題に基づくものである。ＥＣ型は、楕円曲線上の離散対数問題に基づくものである。

## ⓒ　ＲＳＡ暗号

ＲＳＡ暗号は、代表的な公開鍵暗号の１つで、整数論の定理であるオイラーの定理と２つの素数を使って公開鍵暗号の仕掛けを実現しており、大きな数の素因数分解が困難であることを、安全性の根拠としている。インターネットを活用した情報交換では、その相手が不特定多数かつ広範囲となることから、鍵の管理が容易かつ相互運用性に優れた方式が必要になる。ＲＳＡ暗号はその性質を満たしており、ＰＫＩやＳＳＬ、ＴＬＳなど、さまざまな場面で活用されている。

通常の公開鍵暗号方式は、公開鍵を用いて暗号化を行い、秘密鍵を用いて復号を行うが、ＲＳＡ暗号はその構造上、通常の公開鍵暗号方式とは逆に、秘密鍵を利用して暗号化を行い、公開鍵を用いて復号を行うことも可能である。このような性質を電子署名に応用することは十分可能だが、秘密鍵と公開鍵の役割を逆転させたＲＳＡ暗号を、そのまま署名として利用する場合、利用の仕方によっては安全性が損なわれる。このため、ＲＳＡ暗号を電子署名用途に用いる場合には、安全性が証明されているＲＳＡ-ＰＳＳなどの既存の方式を用いるべきである。

**例題演習**

暗号化に関する記述のうち，正しいものはどれか。

ア　ＤＥＳは公開かぎ暗号方式，ＲＳＡは秘密かぎ暗号方式の代表例である。
イ　公開かぎ暗号方式では，必ず暗号化かぎを秘密にして，復号かぎを公開する。
ウ　デジタル署名に利用するには，公開かぎ暗号方式よりも秘密かぎ暗号方式の方がよい。
エ　秘密かぎ暗号方式では，暗号化かぎと復号かぎは同じである。

**解答解説**

暗号化に関する問題である。

アのＤＥＳは秘密鍵暗号方式であり、ＲＳＡは公開鍵暗号方式である。

イは、公開鍵暗号方式では、暗号化鍵を公開する。復号鍵の公開ではない。

ウのデジタル署名に利用するのは公開鍵暗号方式である。秘密鍵方式ではない。

エの秘密鍵暗号方式は、暗号化の鍵と復号の鍵は同じで、求める答えはエとなる。

**例題演習**

通信の“傍受や盗聴”の被害を避ける対策として，正しいものはどれか。

ア　暗号化　　イ　デジタル署名

ウ　ファイアウオール　　エ　メッセージ認証

**解答解説**

傍受や盗聴と暗号化に関する問題である。

アの暗号化は傍受や盗聴されても直ちに内容が把握されることにならないため、被害を避ける対策としては効果がある。求める答えはアとなる。

イのデジタル署名は、発信者の認証である。

ウのファイアフォールは、システムへの不正アクセスの防止である。

エのメッセージ認証は、通信上での情報の改変やエラーの検査のために有効な手段であり、傍受や盗聴防止には役立たない。

**例題演習**

暗号方式に関する記述のうち、正しいものはどれか。

ア　公開かぎ暗号方式では、暗号かぎを通信相手へ秘密裡に配信する必要がある。

イ　公開かぎ暗号方式では、秘密かぎ暗号方式よりも後で考案され、数学的に巧みな理論を応用しているので、秘密かぎ暗号方式に比べ復号処理が単純で高速なものとなっている。

ウ　秘密かぎ暗号方式のかぎを通信の開始時に公開かぎ暗号方式を使って送り、データの暗号化をそのかぎで行うという方法が実用化されている。

エ　秘密かぎ暗号方式は、多数の相手との通信の際、同一の暗号かぎを用いても安全である。

**解答解説**

暗号方式に関する問題である。

アの公開鍵暗号方式は、送信者は受信者の公開鍵を利用して暗号化し、受信者は自分の秘密鍵で復号する。暗号鍵は公開されている。秘密時に配信する必要はない。

イの公開鍵暗号方式は秘密鍵暗号方式と比べて処理方法は複雑なため処理速度も速くはない。単純で高速であるは誤りである。

ウの秘密鍵暗号化方式の鍵管理の方法で、公開かぎ暗号方式を使って復号の鍵を送る方式は実用化されている。求める答えはウとなる。

エの同一の秘密鍵を多数の通信相手に使用すると秘密鍵でなくなるため安全でない。

**例題演習**

データベースで管理されるデータの暗号化に用いることができ，かつ，暗号化と復号とで同じ鍵を使用する暗号化方式はどれか。

ア　ＡＥＳ　　イ　ＰＫＩ　　ウ　ＲＳＡ　　エ　ＳＨＡ-２５６

**解答解説**

共通鍵暗号方式に関する問題である。

アのＡＥＳは、アメリカ合衆国の新暗号規格（Advanced Encryption Standard）として規格化された共通鍵暗号方式である。求める答えはアとなる。

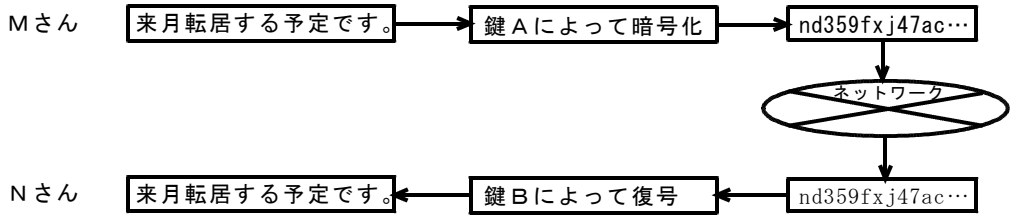
イのＰＫＩは、公開鍵基盤で、公開鍵暗号を用いた技術・製品全般を指す。

ウのＲＳＡは、桁数が大きい合成数の素因数分解問題が困難であることを安全性の根拠とした公開鍵暗号の一つである。

エのＳＨＡ-２５６は、任意長の原文から固定長の特徴的な値であるハッシュ値を求める計算手順である。

**例題演習**

公開鍵暗号方式を用いて、図のようにＭさんからＮさんに他人に秘密にしておきたい文章を送るとき、暗号化と復号に用いる鍵として、適切な組合せはどれか。




| | 鍵Ａ | 鍵Ｂ |
|---|---|---|
| ア | Ｍさんの秘密鍵 | Ｍさんの公開鍵 |
| イ | Ｎさんの公開鍵 | Ｎさんの秘密鍵 |
| ウ | 共通の公開鍵 | Ｎさんの秘密鍵 |
| エ | 共通の秘密鍵 | 共通の公開鍵 |

**解答解説**

公開鍵暗号方式の鍵に関する問題である。

公開鍵暗号方式は、送信元は受信先（Ｎさん）の公開鍵を利用して暗号化し、受信先は（Ｎさん）秘密鍵を利用して復号する。求める答えはイである。

**例題演習**

公開かぎ暗号方式に関する記述として，適切なものはどれか。

ア　ＤＥＳやＦＥＡＬがある。
イ　ＲＳＡや楕円曲線暗号がある。
ウ　暗号化かぎと復号かぎが同一である。
エ　共通かぎの配送が必要である。

**解答解説**

公開鍵暗号方式に関する問題である。

アのＦＥＡＬはＮＴＴが開発した秘密鍵暗号方式、ＤＥＳはＩＢＭ社の開発した秘密鍵暗号方式である。

イのＲＳＡ、楕円曲線暗号は公開鍵暗号方式である。求める答えはイとなる。

ウの暗号化かぎと復号かぎが同一であるのは、秘密鍵暗号方式である。

エの共通かぎの配送が必要なのは秘密鍵暗号方式である。

**例題演習**

公開かぎ暗号方式の暗号化かぎと復号かぎの関係として，適切なものはどれか。

| | 暗号化鍵と復号鍵の関係 | 暗号化鍵 | 復号鍵 |
|---|---|---|---|
| ア | 暗号化鍵≠復号鍵 | 公開 | 公開 |
| イ | 暗号化鍵≠復号鍵 | 公開 | 秘密 |
| ウ | 暗号化鍵＝復号鍵 | 秘密 | 公開 |
| エ | 暗号化鍵＝復号鍵 | 秘密 | 秘密 |

**解答解説**

公開鍵暗号方式の鍵に関する問題である。

公開鍵暗号方式は暗号化鍵と復号鍵は等しくなく、暗号化鍵は公開で、復号鍵は秘密であり、求める答はイとなる。

**例題演習**

暗号化方式の名称に関する記述のうち，共通かぎ方式に分類されるものはどれか。

ア　ＤＥＳ　　イ　ＲＳＡ　　ウ　エルガマル暗号　　エ　だ円曲線暗号

**解答解説**

共通鍵暗号化方式の名称に関する問題である。

アのＤＥＳは米国の商務省標準局によって制定された共通鍵暗号方式である。求める答えはアとなる。

イのＲＳＡは大きな数の素因数分解の困難性を利用したもので、公開鍵暗号方式である。

ウのエルガマル暗号は離散対数問題の困難性を利用したもので、公開鍵暗号方式である。

エの楕円曲線暗号は楕円曲線上の離散対数問題の困難性を利用したもので、公開鍵暗号方式である。

**例題演習**

共通かぎ方式の暗号として，ビット列のデータにかぎとの排他的論理和(Å)を適用する方式がある。排他的論理和とは，次のとおりの結果になる演算である。

0Å0＝0　0Å1＝1　1Å0＝1　1Å1＝0

例えば，１１００というデータに対して，１０１０というかぎを使って暗号化すると，暗号データは０１１０となり，同じかぎとの排他的論理和をとることによって復号もできる。

| | | | | |
|---|---|---|---|---|
| データ | 1 | 1 | 0 | 0 |
| かぎ | 1 | 0 | 1 | 0 |
| 暗号データ | 0 | 1 | 1 | 0 |

↓暗号化　↑復号

１０１０というかぎを使って００１０という暗号データを得た。元のデータはどれか。

ア　００１０　　イ　１０００　　ウ　１０１０　　エ　１１００

**解答解説**

排他的論理和の論理演算によって暗号化する問題である。

元のデータとかぎの１０１０との排他的論理和が００１０となる元のデータを求めればよいことになる。答は１０００となり、求める答えはイとなる。

**例題演習**

ある商店が、顧客からネットワークを通じて注文を受けるために、公開鍵暗号方式を利用して、注文の内容が第三者に分からないようにした。商店、顧客それぞれが利用する鍵の適切な組合せはどれか。

| | 商店 | 顧客 |
|---|---|---|
| ア | 公開鍵 | 秘密鍵 |
| イ | 公開鍵 | 公開鍵と秘密鍵 |
| ウ | 秘密鍵 | 公開鍵 |
| エ | 秘密鍵 | 公開鍵と秘密鍵 |

**解答解説**

公開鍵暗号方式に関する問題である。

顧客から注文内容の秘密を商店が守ることであり、商店の関係者以外に秘密にしなければならないため、商店は秘密鍵、顧客は公開鍵を使用する必要がある。求める答えはウとなる。