公立はこだて未来大学 2021 年度 システム情報科学実習
グループ報告書

Future University-Hakodate 2021 System Information Science Practice
Group Report

プロジェクト名

暗号とセキュリティ

Project Name

Cryptography and Security

グループ名

メールクライアント班

Group Name

Mail Client Team

プロジェクト番号/Project No.

19-B

プロジェクトリーダ/Project Leader

今井徹雄　Tetsuo Imai

グループリーダ/Group Leader

村上光　Hikaru Murakami

グループメンバ/Group Member

今井徹雄　Tetsuo Imai
相馬尚輝　Naoki Soma
廣井悠真　Yuma Hiroi
村上光　Hikaru Murakami
山端祐輝　Yuki Yamahata

指導教員

白勢政明　由良文孝

Advisor

Masaaki Shirase　Fumitaka Yura

提出日

2022 年 1 月 19 日

Date of Submission

January 19, 2022

概要

本プロジェクトは、暗号化技術という観点からセキュリティに関する理解を深め、実際に活用・体験することを目的としたプロジェクトである。主に昨年度から新型コロナウイルスの影響により、オンライン授業やリモートワークの増加に伴って情報の管理が以前より重要となっている。そこで、情報を守るセキュリティ技術や、それを扱うユーザのセキュリティ意識がより大切になる。今年度のメール班での活動は、セキュリティ技術や攻撃手法について学習し、私達を守る技術である暗号化技術のより効果的な利活用について考え、さらに実際のメールシステムに実装することを目標として活動する。

キーワード　セキュリティ, ID ベース署名, タイムリリース暗号, 高機能暗号

（文責: 今井徹雄）

Abstract

This project's purpose is to deepen the understanding of security in terms of cryptographic technology and actually to utilize and experience it. Information management has become more important than before due to the increase of online lessons and remote work mainly influenced by COVID-19 since last year. Therefore, security technology that protects information and security consciousness that the user handles become more important. This year mail group activity learns about security technology and attack methods and thinks about more effective use of cryptographic technology. In addition, we will work with the goal of implementing it in an actual mail system.

Keyword Security , ID-Based signature , Timed-Release Encryption , Cryptography with Advanced Functionality

（文責: 今井徹雄）

目次

第 1 章　背景

1.1　背景

主に昨年度から新型コロナウイルスの流行により、インターネットを介した電子メールの利用が増加している。電子メールの使用における利点として、遠く離れている相手や、直接会えない相手との意思の疎通や情報の共有がしやすいという点が挙げられる。しかし一方、このような電子メールにおいて、情報の改ざんや内容の盗聴、なりすましといった危険性があり、電子メールの利用の増加とともに今後もその被害は増加していくだろう。また、このような危険性のある攻撃の一つは「標的型攻撃」と呼ばれており、これは関係者を装うことで電子メール等に添付されたウイルスを用いて組織や個人のシステムを攻撃することである。情報処理推進機構によって行われた情報セキュリティに対する意識調査 [1] でも標的型攻撃に注目していることからもこの攻撃の脅威は明らかである。これに対して知名度が低いという点がこの調査からこの攻撃の特徴として挙げられる。

こうした電子メールの脅威に対して人的対策の他に、技術的対策として攻撃者にメールの内容を容易に読み取られないように、一見して意味のない文字列に変換してデータを通信する暗号化技術を応用することで攻撃を防止している。この暗号化技術の発展技術として、高機能暗号というものがある。しかし、高機能暗号の性質として有効に実装できる機能や状況が限られており、実際にどういった部分の利活用を考えられるかについてが課題であり現状である。

（文責: 今井徹雄）

1.2　目的

本プロジェクトの活動では、比較的小規模である学内メールシステムに高機能暗号を実装することで、電子メールの危険性の防止や高機能暗号の利活用について考え、検証することを目的とする。ここで用いる高機能暗号として ID ベース暗号とタイムリリース暗号とした。ID ベース暗号は、学内メールシステムのような小規模なメールシステムにおいてメールアドレスの認証が容易なことから、有効に安全性を保ちやすいという特徴があり、またこれを用いた電子署名を実装することで情報の改ざんやなりすましを防止できると考えられる。また、タイムリリース暗号は、指定時間以前に復号できないようにすることで安全性を有効に保てるという特徴があり、これをメールの時間限定公開のような機能として実装することで、送信者の意図しない時間における内容の盗聴を防止できると考えられる。

過去の卒業生の研究では、ID ベース暗号とタイムリリース暗号の両暗号方式とも学内メールシステムに対してメッセージの暗号化・復号における正当性や完全性の検証が行われていた。[2] また、従来の対策法として後述する S/MIME という電子証明書の技術がある。対して、高機能暗号はこうした問題の対処をした上で、先述した標的型攻撃を防ぐ手段として活用することが可能である。本プロジェクトでは、こうしたメールシステムにおける安全性確保を、暗号化技術を通して考え、実装することで必要な技術や問題点を検証することを目的とする。

（文責: 今井徹雄）

1.3 従来例とその問題点

標的型攻撃に対する従来の対策法として S/MIME(Secure/Multipurpose Internet Mail Extansions) という電子メールに対する暗号化方式がある。これは電子証明書の技術を用いてメールの暗号化や電子署名を行うことが出来、通信の秘匿やなりすましの検知に対して活用することが出来る。しかし、この導入には以下のような問題点がある。

- コストが高い
- 送信者受信者の両方が S/MIME に対応している必要がある
- 認証局の存在が必須である

S/MIME は信頼できる第三者機関からその証明書を発行して貰う必要があり、GMO グローバルデサイン株式会社 [3] によるライセンスでは、1 つにつき有効期限 1 年で税込 57200 円の費用がかかり、それをもし学内メールシステムに使用する場合は全利用者にそれを適用する必要があるため多額の費用がかかってしまう。

また、S/MIME を全員が使用するためには全員がそれに対応するメールソフトを使用する必要があり、メールの送信者と受信者が S/MIME を使用できる環境でないと意味がない。また、先述した通り証明書には有効期限があり、その有効期限が切れる度に利用者は証明書を更新をしなければいけないという問題点がある。

加えて、電子証明書の発行や検証を行う第三者機関である認証局 (Certification Authority) が必須であるという点がある。S/MIME では受信者が送信者の公開鍵を使ってその署名検証を行う関係上、その公開鍵が本当に信頼できるのかを証明してくれる認証局の存在は必要となっている。

（文責: 今井徹雄）

1.4 方針

上記の目的を達成するため、ID ベース暗号を用いた ID ベース署名、ID ベース暗号を用いたファイルの暗号化機能、タイムリリース暗号を用いたファイルの時間指定公開機能の 3 つを実装方針とした。ID ベース暗号とは、ID という例えばメールアドレスや学籍番号といった個人を示すことが出来る識別子を元に公開鍵を生成する公開鍵暗号方式である。これを用いた署名方式が ID ベース署名である。また、この ID の代わりに時刻を用いることで、決められた時刻になるまでは復号できないことを保証する暗号方式がタイムリリース暗号である。

また、学内メールシステムは利用者の大半が学生であり、利用しているメールアドレスには学籍番号等が使われているため、メールアドレスから個人との紐付けが容易であることから ID を使用することが有効であり、この機能を有したメールシステムを実装することで学内メールシステムにおける通信において標的型攻撃に対する有効な対策となる。また、メールシステムとしてタイムリリース暗号を時間に関わる機能として実装することで、そのシステムに沿った暗号機能の実装を考える。

ID ベース暗号は公開鍵に個人を示すことが出来る ID を使用するため、従来例のような公開鍵が有効であることを証明する電子証明書が不要であり、またこのことより第三者機関である認証局が不要となるため、S/MIME 証明書にかかるコストを削減できる。加えて、学内メールシステムの

ような全利用者が一つのメールシステムを使用しているとわかっている場合、このメールシステムに暗号機能を実装することで先述した従来例に存在する問題点の対処が可能であることがわかる。

また、比較的小規模なメールシステムに対して Google Chrome 拡張を用いて実装することで、学内メールシステムへの実装を容易にし、電子メールの危険性に対する暗号化技術の利活用という目的の達成を目指した。

（文責: 今井徹雄）

第 2 章　プロジェクトに関する基礎知識

2.1　暗号

暗号とは、一定の規則に従って文章・数などを他の表現に変えて、第三者に元の文章・数が何かをわからなくすることである。暗号には様々なアルゴリズムが存在するが、それらの暗号アルゴリズムは一般に、機密性、完全性、認証を目的として使用される。

機密性　データを認可されない窃取から保護することで、情報保護のために使われる。セキュアな暗号アルゴリズムであれば、共通鍵又は秘密鍵を持つ認可された当事者のみが暗号文をもとの文に復号できる。

完全性　データを認可されない改ざんから保護することで、改ざん検知・メッセージ認証のために使われる。後述する公開鍵を用いたデジタル署名を用いることで、データ改ざんを当該データの使用前に検出できる。

認証　データの送信元が正しいところから来たものであるか確認したり、その送信元が正しいかを確認したりするために使われる。暗号アルゴリズムを使ったセキュアな認証方法やデジタル署名であれば、正当な送信元であるかを使用前に検出できる。

暗号化の方式には、次々と新しい方式が提案され、また、用途によっても異なる暗号方式が採択される。これらの暗号方式には、様々な区分の仕方がある。その中でも代表的なものとして、共通鍵暗号方式 (2.2.1) や公開鍵暗号方式 (2.2.2) がある。

（文責: 相馬尚輝）

2.2　暗号方式

2.2.1　共通鍵暗号方式

共通鍵暗号方式とは、送受信者間で同一の鍵を用い、暗号化・復号を行う技術である。対称鍵暗号方式とも呼ばれる。共通鍵暗号方式には次のような特徴がある。

- 平文を暗号に変換するときと暗号を平文に変換するときのルールと鍵が同一である。
- 送信者と受信者は同じ鍵を持つ。これは共通鍵と呼ばれる。
- 通信相手が増えるごとに管理する鍵の数が増え、鍵管理の負担が大きくなる。
- 秘密鍵の配布方法が手間になる。

代表的な実装方式として AES がある。AES は特定の長さのブロックを単位として処理を行う「ブロック暗号」の一つであり、128、192、256 ビットの 3 通りの長さの鍵を利用できる。他にも、携帯電話機等の小型で処理能力が限られた機器や大容量データの高速処理向けに開発されたストリーム暗号である、KCipher-2 がある。

（文責: 相馬尚輝）

2.2.2 公開鍵暗号方式

公開鍵暗号方式とは、送受信者間で「公開鍵・秘密鍵」と呼ばれるペアの鍵を用い、暗号化・復号を行う技術である。公開鍵暗号方式には次のような特徴がある。

- 公開鍵は、広く一般に公開し、誰でも使用できる。
- 秘密鍵は、受信者のみが使用するので、受信者だけが暗号化された文書を復号しても読むことができる。
- 受信者は、送信者が増えても秘密鍵を 1 つ持っていればよいので鍵管理の負担が少ない。
- 共通鍵暗号方式に比べて処理が遅い。

この方式は、前述した共通鍵暗号方式の問題点である「鍵配布の方法」、「鍵管理負担」の 2 つを同時に解決できる。しかし、メッセージの改ざんやなりすましを防止するためには鍵を証明するための機関である公開鍵基盤が必要である。代表的な実装方式として大きな数値の素因数分解に膨大な時間がかかることを安全の根拠とする RSA がある。他にも離散対数問題の困難性を安全の根拠とする楕円曲線暗号や ElGamal 暗号がある。これらの公開鍵暗号方式を応用したものにデジタル署名がある。

（文責: 相馬尚輝）

2.3 電子署名

電子署名とは電子化された文章に対して行われる電子的な署名なことである。インターネット上の電子化された文章は第三者によって改ざんや内容の盗聴、なりすましなどのリスクが存在する。電子署名はこのようなリスクを防止するための有効な手段となりうる。本プロジェクトでの電子署名とは公開鍵暗号方式を用いたデジタル署名のことを指す。電子署名は送信者、受信者間で次のような手順で行われる。

1. 送信者は自分の秘密鍵で電子文書を暗号化と同様の処理をし電子署名を生成する。
2. 送信者は電子文書と電子署名を組みにして検証者に送る。
3. 受信者は受け取った公開鍵で電子署名を復号し、その結果と電子文書を比較する。
4. もしそれら二つが一致していれば受け取った電子署名は送信者の秘密鍵で署名生成されたことが保証される。
5. 受信者は送られた電子文書が送信者本人であるということが確認できる。

上記の手順で電子文書を送受信する際には公開暗号方式を使用しているため処理速度が遅いという欠点があげられる。実際に署名を行う際には暗号学的ハッシュ関数という関数を使用しデータを圧縮することで処理速度を向上させることができる。暗号学的ハッシュ関数とは簡単にデータを一文字でも変えると出力が変わり、衝突を予測することが難しい関数である。

（文責: 相馬尚輝）

2.4 高機能暗号

高機能暗号とは従来の暗号技術に高度な機能を付加した暗号技術である。高機能暗号にはデータを暗号化したまま検索する暗号技術である検索可能暗号 [4] や、受信者の公開鍵を用いて暗号化した暗号文を、第三者の秘密鍵を用いて復号が可能となるよう代理人が変換する代理再暗号化 [5][6] が挙げられる。後項では本プロジェクトで利用した高機能暗号である ID ベース暗号とタイムリリース暗号を紹介する。またこれらの暗号は双線形性ペアリングを用いた楕円曲線暗号であるため、次項ではペアリングを数式を用いて説明する。

（文責: 相馬尚輝）

2.4.1 ペアリング

ここからはペアリングについて数式を用いて説明する。G_1,G_2 を加法に関する巡回群, G_3 を乗法に関する巡回群とする。

$$e : G_1 \times G_2 \to G_3$$

上記の写像 e が次の (1) 双線形性と、(2) 非退化性を満たすとき、e はペアリングと定義される。

(1) G_1 の任意の二点 P,Q、任意の整数 a,b に対して次の関係式を満たすことを、双線形性という。

$$e(aP, bQ) = e(P, Q)^{ab}$$

(2) $e(P, P) \neq 1$ となる $P \in G_1$ が存在したとき、これを非退化性という。

特に、(1) の性質より、次の数式が成立する。

$$e(aP, bQ) = e(P, Q)^{ab} = e(bP, aQ)$$

上記の式が $G_1 = G_2$ の時には対象ペアリング、$G_1 \neq G_2$ の時には非対称ペアリングと呼ばれる。非対称ペアリングは特に計算処理速度が速いことから、研究で用いることが多くなっている。

（文責: 相馬尚輝）

2.4.2 ID ベース暗号

ID ベース暗号とは公開鍵に個人を特定できる情報である ID（Identifier）を使用し、その ID を元に秘密鍵を生成する暗号方式である。ここでの個人を特定できる情報とは、メールアドレス、携帯電話の番号、基礎年金番号等のような公開性の高い情報である。また双曲線ペアリングを用いた楕円曲線暗号である。ID ベース暗号は、従来の公開鍵暗号方式で必要とされた公開鍵基盤が不要であることや、先に秘密鍵がなくても公開鍵を用いて暗号化できるという特徴が挙げられる。以下では、ID ベース暗号を数式を用いて説明する。簡単にするためにこれ以降はメッセージの送信者を Alice、受信者を Bob と表記する。

セットアップ

1. 楕円曲線 E/F_q において,$E[n] \subset E(E_{q^k})$ があるとする。
2. PKG はマスター鍵 $s \in Z_n^*$ を選択する。また $P \in E[n]$ を選び、$Q = sP$ を計算して P と Q を公開する。なお、マスター鍵は一定期間変更しない。
3. ハッシュ関数 H_1, H_2 を選び、公開する。

$$H_1 : \{0,1\}^* \neq E(F_p), \quad H_2 : F_{q^k} \to \{0,1\}^n$$

4. 公開鍵を $P_A = H_1(ID)$ とする。

秘密鍵生成

Bob の秘密鍵を $S_A = sP_A$ とする。

暗号化

Alice は公開鍵 P_A を用いて、暗号文 C を生成する。また、乱数 $x \in Z_q^*$ を選択する。

$$C = (C_1, C_2) = (xP, m \cdot H_2(e(P_A, xS_A)))$$

復号

Bob は秘密鍵 S_A を用いて、暗号文 C を復号する。

$$m = C_2 / H_2(e(S_A, C_1))$$

（文責: 相馬尚輝）

2.4.3 タイムリリース暗号

タイムリリース暗号とは ID ベース暗号の ID に時刻情報を用いる暗号方式である。2.4.2 節で述べたように、先に秘密鍵がなくても公開鍵を用いて暗号化できるという特徴を用いて、指定された時刻にならなければ秘密鍵を生成しないことでその指定された時刻までの安全性が保障されるという利点がある。先行研究としてこのタイムリリース暗号に関して学内メールシステムに実装する際に正当性が保たれることが確認されている [2] ため、タイムリリース暗号を学内メールシステムに実装することにした。以下では、タイムリリース暗号を数式を用いて説明する。

セットアップ

1. 楕円曲線 E/F_q において、$E[n] \subset E(E_{q^k})$ があるとする.
2. PKG はマスター鍵 $s \in Z_n^*$ を選択する。また $P \in E[n]$ を選び、$Q = sP$ を計算して P と Q を公開する。なお、マスター鍵は一定期間変更しない。
3. 次のようなハッシュ関数 H_1, H_2 を選び、公開する。

$$H_1 : \{0,1\}^* \to G_1, \quad H_2 : G_2 \to \{0,1\}^n$$

4. 公開鍵を $P_T = H_1(TIME)$ とする。(TIME は復号時刻を文字列にしたもの)

時間鍵生成

時間鍵を $K_T = sP_A$ とする。

暗号化

Alice は公開鍵 P_A を用いて、暗号文 C を生成する。また、乱数 $x \in Z_q^*$ を選択する

$$C = (C_1, C_2) = (xP, m \cdot H_2(e(P_A, xS_A)))$$

時間鍵配布

時間鍵生成局は復号時刻になったら Bob に時間鍵 T_T を配布する。復号

Bob は時間鍵 T_T を用いて暗号文 C を復号する。

$$m = C_2 / H_2(e(T_T, C_1))$$

（文責: 相馬尚輝）

第 3 章　到達目標

3.1　問題設定

最も警戒するべき組織向け脅威として「標的型攻撃」が存在する。しかし、既存の対抗技術である電子署名は認証局による公開鍵認証サービスを契約する必要があるため年間コストが高い。送信者と受信者の両方のメールクライアントが対応している必要があるにも拘わらず、相手のメールクライアントが対応しているか判らないことなどからあまり普及していない。そこで本グループでは、電子署名導入の障害となっている上記 2 つの理由「年間コストが高いこと」「相手のメールアドレスが電子署名に対応しているかわからないこと」に着目した。電子署名は、その文書ファイルが第三者の手によって改ざんされていないことを証明する物である。現実の紙書類の印鑑やサインのような証明をする役割がある。印鑑やサインのような役割を果たすためには、その署名が正しいものであると証明する必要がある。そのためには認証局がその署名が正しいことを証明するできるようにするために、電子証明書と確認を行うことを必要とする。電子署名は「電子署名及び認証業務に関する法律」で基準が定められている。通常の電子メールは送信者と受信者の間に第三者が割り込み、なりすましや電子メールの改ざんを行うことが可能になっており、そのなりすましや改ざんによって悪意あるテキストやウィルス等のファイルを送ることが可能になってしまう。具体的には、受信者から信頼できる送信者本人を名乗ったテキストメールを送り、金銭を扱うサイトへ誘導することができてしまう。その対策として、ハッシュ値を用いた電子署名を使うことができる。送信者の認証を行うことで本人の証拠が残るため、メールを偽装して送信者を偽るなりすましも検知することができる。電子署名のシステムを作成する上で、鍵の受け渡しのためのユーザーごとの認証機能が必要になる。ユーザー認証システムは新規に作成する上では難易度が高い。そこで、web サービス上にある認証システムとして Firebase の認証機能である Firebase Authentication を使用することとした。ログインシステムを使用することによって明確に送信者、受信者本人であることを確認し、より安全に鍵やトークンの受け渡しを可能とした。電子署名は、送信者は送信する本文を秘密鍵とハッシュ化を用いて署名を生成し、本文と一緒に送信する。受信者側は公開鍵と一緒にその署名を検証して得たハッシュ値と本文をハッシュ化したものを比較する。電子署名に関連した暗号技術として ID ベース暗号がある。ID ベース暗号は公開鍵にメールアドレスのような本人であることを示すことが出来る ID を使用し、秘密鍵は同様の ID を元に生成する。ID ベース暗号のように通常の暗号技術に加えて高度な機能を追加したものを高機能暗号と呼ぶ。高機能暗号の一つとして、時間を指定できる機能を加えたタイムリリース暗号がある。これは送信者が受信者の復号できる日時を指定することができる。また、先行研究 [2] によりタイムリリース暗号に関しての正当性が 100 年分保たれることが確認されている。このような暗号機能・電子署名が普及していないことから標的型攻撃の対策技術として十分な機能を満たせていないことを問題として設定した。

（文責: 廣井悠真）

3.2 課題設定

去年のプロジェクトでは標的型攻撃の対抗技術として存在する電子署名の普及が目標であった。電子署名は年間コストが高いこと、相手のメールアドレスが電子署名に対応しているかわからないことなどから普及しておらず、標的型攻撃の対抗技術として十分な機能を満たせていない事が問題であった。電子署名が普及していない原因である年間コストを減らすため、運用コストの低い ID ベース署名を搭載したメールクライアントを作成した。今年度は昨年度の目標を更に発展させ、コロナの影響によって起こるセキュリティ問題を解決することにした。そこで、現環境における新たな問題を見つけ出すためメンバーと議論した。その結果、このコロナ禍での選挙で投票所に集まると密になってしまう問題をタイムリリース暗号を使ってオンライン投票をできるようにしたいと考えた。投票は国民の大事な物であり、重大な個人情報でもある。オンライン上の投票と比べると、物理的な投票では第三者的な立場である立会人が投票所に必ず居て、投票に不正がないかの確認を行い、投票した人が人を偽ってないかの本人確認が行われる。オンライン上でそれらのチェックを行い、偽装が無いかの確認を行う必要がある。電子署名ではそれらの確認を行うことが出来る。第三者からの介入を防ぐために暗号を用いる必要がある。投票はある一定の時間に達するまでは、その内容を開く必要性がなく、更に時間になったら一斉に内容を開く必要性がある。これらの要件を満たすことができる可能性があるのがタイムリリース暗号である。タイムリリース暗号は暗号文を作成し、送信した後、指定したある時間になったらその時間を鍵とする時間鍵を送る暗号システムである。未来大学の以前の卒業論文にタイムリリース機能の正当性を確認したものがある。そこで、本グループでは、タイムリリース暗号を利用できるメールシステムを作成することを目的として活動していくことになった。

標的型攻撃は情報セキュリティ上の脅威となりうる攻撃であり、対策すべき物である。標的型攻撃では企業などの大規模なものに対する攻撃ではなく、一個人を狙った攻撃法である。具体的には、なりすましや改ざんを行い、受信者本人を油断させ、攻撃に使うファイルを開かせる方法である。この方法は、受信者にとって警戒する手段が少なく、事前に確認を行わない限り防ぐ手段が少ない。攻撃に使うファイルの中にはランサムウェアが仕込まれる可能性がある。ランサムウェアはファイルを勝手に暗号化し、もとに戻すことと引き換えに金銭を要求するものである。コンピュータはもはや人類にとって欠かせないものであり、パソコンや日常的に所持するスマートフォンの中には大量の個人情報がある。一個人のデータだけでなく企業の顧客管理や機密情報を扱うパソコンだった場合、情報を公開されてしまうと大変なことになってしまう。これらの心理を用いて身代金を要求するものである。ランサムウェアは身代金を払うと解除されるものが多い。ランサムウェアの目的はデータの取得ではなくあくまでも金銭であり、金銭を払えばデータが帰ってくると主張し、実際にデータが帰ってくれば金銭を払ってもらえる可能性が高い。ランサムウェアに対して身代金を払うことは推奨されていない。このようなランサムウェアにかからないために事前にセキュリティの強化を行う必要がある。電子署名ではメールに付属して、なりすましの防止やデータ改ざん検知を行う暗号技術である。電子署名は公開鍵暗号の処理と類似しており、それらの知識を使うことが出来る。メールでの電子署名が普及すれば、標的型攻撃によるランサムウェアなどの攻撃を事前に防ぐことが出来る。

暗号のシステムを構築するに当たり、前期では担当教員による暗号に関する講義を受けた。内容は主に、暗号に関する知識の会得であった。実在する暗号方式を例に取り、シンプルな暗号システムからはじめ、プロジェクトに使う暗号の学習をした。シーザー暗号は簡単な暗号の一つである。

シーザー暗号は原文である文字のアルファベットをある一定数ずらし、読めなくする暗号である。これは暗号化が簡単であり便利だが、それと同時に復号のための動作が読みやすく、暗号を解読されやすい弱点がある。プログラム上では、まず乱数を作成し、その乱数によって文字をずらす量を決める。計算には mod を用いた計算を行い、復号を行えるようにしている。復号のための key を複数個作成することも出来る。鍵の受け渡しを行うために鍵配送問題がある。メールを暗号化し、復号する上で送信者が受信者に対して鍵を送らなければいけない。しかし、鍵をメールで送ってしまうと、その鍵を見られてしまったら本末転倒になってしまう。その問題を解決したのが公開鍵暗号である。復号と暗号化の鍵が違い、公開鍵と秘密鍵を作成する。送信者は受信者から予め公開鍵を受け取り、送信するメールにその鍵を使って暗号化しメールを送る。受信者は秘密鍵を使用して復号することが出来る。このような鍵システムを用いる。

具体的な機能の構成としては、ID ベースには送受信者やメールサーバ以外にも鍵生成局と認証局というものがあり、認証局とは送られてきたトークンが本人のものかを認証するものである。鍵生成局は送信者には暗号化のための秘密鍵を渡し、受信者には復号のための公開鍵を渡す役割である。タイムリリースの構成は、認証局が無く、時間鍵が復号時刻まで渡さないためである。ユーザー情報を登録し、ID ベース署名をクライアント上で生成し、受信者側が署名の検証を行う。サーバーでは生成した鍵を送信者と受信者の間で受け渡しを行う。その際にユーザー情報に誤認がないかのチェックを行う。ユーザーの認証には Firebase を用いたログイン認証システムを使用した。Firebase Authentication を使い、web サイト上でユーザー情報の新規登録、ログインを行えるようにする。ユーザー情報、ログイン情報はすべて PostgreSQL 上で管理され、誤認を起こさないようにする。JWT を用いたチェックによって、より強固な認証システムを構築する。

これらのシステムの作成を目標課題とした。

（文責: 廣井悠真）

3.3　到達レベル・具体的な手順

タイムリリース暗号・ID ベース暗号機能を用い、ファイルの暗号化と署名生成ができる機能をメールシステムに実装することを目標にした。機能の実装をするにあたり、クライアント側とサーバ側の二つにチームを分けた。また、昨年の本プロジェクトではファイルの暗号化・復号をメールシステムと別のサイトを用いていたため、それを改善し、メールの送受信の時点で暗号化と復号をできるようにした。

前期活動には暗号の知識を深めるために講義を行い、それに加えてクライアント側では後期活動までの課題として各々で任意の言語を用いて暗号機能を実装し、サーバ側では各自で実装に必要な知識を身につけた。後期活動に入り実装機能の分担・開発を行いそれぞれの機能の統合を行った。

（文責: 山端祐輝）

3.4　スケジュール

前期の活動は 5 月から 8 月にかけて行われた。5 月はメンバーをメール班と WEB 班に分けて、それぞれの活動を行った。また、プロジェクト担当の教授から暗号に関する基礎知識を習得するための講義を受けた。講義はオンライン形式で行い、シーザー暗号を始めとした基礎的なものか

ら学んだ。6 月はその講義で得た知識を元に、前回のプロジェクトや卒業研究生の論文を参考にして暗号システムの理解を深めた。中間発表の準備のため、スライドの作成や発表のためのポスターの作成を行った。7 月は実装する機能の方向性を決め、班内でチーム分けを行い、クライアント側とサーバー側に分けた。中間発表を行い、参加者から受けた指摘をまとめ、今後の参考にした。後期の活動は 10 月から 1 月にかけて行われた。10 月は前期に習得した知識を元に成果物の作成に着手した。詳細的な機能の制定を行い、ID ベース署名と ID ベース暗号を用いたファイルの暗号化とタイムリリース暗号を用いたファイルの暗号化を行うことにした。Firebase の機能である Firebase Authentication を用いたログイン認証機能の作成を行った。11 月 12 月は各機能の制作を行った。Google Chrome 拡張機能に対する実装を始めた。サーバ側では引き続き必要知識の習得をし、サーバーを実装しアプリケーションを動かすために Amazon Web Servise を利用した。データベースの管理のために PostgreSQL を利用した。成果発表会に向けた、成果物の作成、発表のためのスライドの作成、ポスターの作成、発表用の動画の作成を行った。成果発表会で受けた指摘をリストアップし、それをもとに改善を行った。1 月は後期末提出物の作成を行った。

（文責: 廣井悠真）

- 前期

  5 月　メンバーの班決め、暗号の基礎知識の習得、担当教員による暗号の講義

  6 月　前回プロジェクトや卒業研究生の論文を参考に暗号システムの理解を深める、作成する機能の制定、中間発表準備

  7 月　班内での実装担当をクライアント側とサーバー側にチーム分け、中間発表

  8 月　必要知識の習得、プログラムの理解
- 後期

  10 月　実装する機能の詳細の制定、メンバーごとの役割の割り当て

  11 月　プログラムの作成、サーバーの構築

  12 月　成果発表に向けた成果物の作成、成果発表の準備

  1 月　　後期末提出物の作成

（文責: 廣井悠真）

3.5　前期活動

ID ベース暗号・タイムリリース暗号機能を搭載したメールクライアントを作成し、問題なくメール本文及び添付ファイルの送受信ができることを目標とした。なお、開発環境は Visual Studio Code を用い、開発言語は Javascript を使用した。作成するメールクライアントはハイブリッド暗号方式を採用し、添付ファイルの暗号化には OpenSSL の AES を用いた。また、共通鍵の暗号化と電子署名には ID ベース暗号を用いる。

（文責: 山端祐輝）

3.5.1　ID ベース暗号の暗号化手順

暗号化の手順を以下に記載する

1. 平文を.txt 形式で保存する
2. ファイルからハッシュ値を計算する
3. ハッシュ値を ID ベース暗号の秘密鍵で暗号化する
4. 暗号化されたハッシュ値を平文の.txt ファイルの文末に追加する
5. 手順 2〜手順 4 を添付ファイル分繰り返す
6. 共通鍵を生成する
7. 平文を共通鍵で暗号化する
8. 添付ファイルを共通鍵で暗号化する
9. 共通鍵を ID ベース暗号の公開鍵で暗号化する
10. 暗号文に暗号化された共通鍵を付ける
11. 暗号文を読み込む
12. 暗号文・暗号化された添付ファイルを送信する

（文責: 山端祐輝）

3.5.2 ID ベース暗号の復号手順

復号の手順を以下に記載する

1. 暗号文を.txt 形式で保存する
2. 暗号文の文末から暗号化された共通鍵を読み込む
3. 暗号化された共通鍵を ID ベース暗号の秘密鍵で復号する
4. 暗号文を共通鍵で復号する
5. 暗号化された添付ファイルを共通鍵で復号する
6. ファイルの文末からハッシュ値を読み取る
7. ファイルからハッシュ値を計算する
8. ハッシュ値を比較する

（文責: 山端祐輝）

3.5.3 タイムリリース暗号の暗号化手順

暗号化の手順を以下に記載する

1. 平文を.txt 形式で保存する
2. 共通鍵暗号の鍵をランダムに選ぶ
3. 平文を共通鍵で暗号化する
4. 復号してほしい時刻の文字列を公開鍵として共通鍵を暗号化する
5. 暗号化された平文と暗号化された共通鍵を送信する

（文責: 山端祐輝）

3.5.4　タイムリリース暗号の復号手順

復号の手順を以下に記載する

1. 暗号文を.txt 形式で保存する
2. 決められた時刻になったら時刻鍵生成局によって公開される時刻鍵を用いて共通鍵を復号する
3. 共通鍵を用いて暗号化された平文を復号する

（文責: 山端祐輝）

3.6　課題の割り当て

各人の興味のある分野及び関連性、時間軸のスケジュールを基準に以下のように割り当てた。

1. クライアント班（今井・相馬・山端）
   ＜タイムリリース暗号＞
   　ID と時刻情報を公開鍵としてメッセージを暗号化して送信する
   ＜ ID ベース暗号＞
   　メールアドレス等の ID を公開鍵としてメッセージを暗号化して送る

2. サーバ班（廣井・村上）
   ＜タイムリリース暗号＞
   　ある時刻になったら秘密鍵を発行し、メール受信者に暗号文を復号させる
   ＜ ID ベース暗号＞
   　メールアドレス等の ID をもとに作成された秘密鍵を発行し、メール受信者に暗号文を復号させる

（文責: 山端祐輝）

3.7　前期活動のフィードバック

プロジェクト全体の活動として暗号についての知識を深めた。本グループでの前期の活動として、昨年の本プロジェクトで行われていたコードの改善をして ID ベース暗号とタイムリリース暗号を用いたメールクライアントを作成し、問題なくメール本文及び添付ファイルの送受信ができることを目標とした。なお、開発環境は Visual Studio Code を使用した。前半の活動では電子署名の仕組みを先生の講義や先行研究として卒研生の論文を読むなどして理解した。また、実際に昨年の本プロジェクト生に依頼し、実際に昨年のプログラムの解説をしてもらい、プログラムに対して理解を深めて今後の活動について実装方法を考えた。その後、クライアント側では知識の定着の一環で後期活動までの課題として各々で任意の言語を用いて暗号機能を実装し、サーバ側では各自で実装に必要な知識を身につけた。そのため、実際の開発は後期活動期間中に行うこととなった。また、中間発表についてはスライドや発表内容に関しては好評であったが、質問のなかった時に無言

の時間があり空白の時間が生まれていたことが反省点であった。そのため、後期はこの反省を生かすことをプロジェクト全体で共有した。

（文責: 山端祐輝）

3.8　後期活動

後期の活動にあたって、まず始めに各々に割り振られたプログラムを完成させることとした。それが完成した後、プログラムを統合することとした。それにあたり、関数や変数の名前を統一するようにコードを書き換える。また、統一する際には Github を用い、スムーズにコードの統一を行えるようにした。すべての統合が終わった後、発生したバグやエラーなどを取り除きプログラムの完成を目指した。

（文責: 山端祐輝）

3.9　後期活動のフィードバック

後期の活動では、各々に割り振られたプログラムの完成を目指すところから始まった。また、いち早く自分のプログラムを完成させたものは、Chrome に実装するために必要なコードを記述した。全員がプログラムを完成させた後、プログラムの統合を行った。その後、プログラムに発生した多少のバグや細かな誤植を修正した。

最終発表では前期の反省点を生かし、空白の時間を作らないように構成を変えた。最初に質疑応答をし、質問がなかった場合にスライドの解説をしつつ、質問を募集した。その結果、空白の時間をなくし、発表の構成については好評であった。しかし、理解が難しかった人も少なからずおり、スライドを初見の人でもわかりやすくする必要があることを反省点とした。

（文責: 山端祐輝）

第 4 章　プロジェクト内のインターワーキング

4.1　今井徹雄

前期

学内メールシステムに暗号化技術を実装するにあたって、必要な知識や開発環境、必要となるツールや設計方針などの情報をグループメンバーに共有した。また、自身で作成した電子署名に関するプログラムを共有することで、グループ全体の成果物に対する理解を促した。

プロジェクト学習中間発表の準備においては、プロジェクトメンバーにポスターやスライド作成などの役割を割り当て、コンテンツのフィードバックを主体的に行うことで、中間発表資料の見やすさやわかりやすさの向上に努めた。

後期

メール班をグループに分割後、担当したクライアント班にて各個人機能ごとに実装を分担して完成を目指すとともに、Google Chrome 拡張機能への対応に合わせた実装に関する注意喚起や各機能のプログラムを統合する際の方法を共有した。

プロジェクト学習成果発表会の準備においては、中間発表時と同様にポスターとスライド作成に関する役割を割り当て、それらのフィードバックを主体的に行った。加えて、中間発表の際に判明した発表方式の問題点を明確にしてそれらを解決するためにどうしたらより良い発表になるのかを考えて共有し、発表自体の向上に努めた。

（文責: 今井徹雄）

4.2　相馬尚輝

前期

プロジェクトの方針や仕事の割り当てを決める際には積極的に話し合いに参加し、進行することができた。また、作業を効率化するためのツールの提案や普段から作業報告をすることでチームの作業を円滑に進めるためのサポートをした。暗号の理論もプロジェクト時間なだけでなく時間外の学習をしそれらをチームメンバーとの話し合いの際にも役立たせることでチームとしての目標を明確に設定することができた。中間発表の際には、作成するスライドや原稿、ポスターの修正から音声、動画編集、質疑応答など複数の担当を担いグループとしても貢献することができた。

後期

最終成果物であるメールシステムの ID ベース署名と検証のプログラムを作成した。成果物の作成の際にはメンバーとツールの使い方を共有したり、成果物に対するレビューを行うことで見える部分と見えない部分の両方から直接的にも間接的にも貢献をすることができた。

最終成果発表では、前期に引き続き作成するスライドや原稿、ポスターの修正から音声、動画編集、質疑応答など複数の担当を担いグループとしても貢献することができた。

（文責: 相馬尚輝）

4.3 廣井悠真

前期

はじめは暗号システムの知識を習得するために、担当教員からの暗号に関する講義を受けた。その講義で得た知識を元に、過去のプロジェクトや卒業論文を参考にしてより知識を深めた。サーバサイドの環境を構築するにあたって、サーバについての基礎知識や firebase を使ったメールシステムの機能の開発をメンバーと協力し行った。サーバーを扱う上で必要なプログラムの学習を行った。中間発表の準備において、発表の動画を作成する際に使うスライドの作成を行った。スライドの作成時はメンバーからの指摘やアドバイスをもらいわかりやすいスライドの完成を目指した。

後期

学内メールシステムに ID ベース署名・暗号のサーバーの担当を行った。引き続き Firebase の認証システムを使ったログインシステムの作成を行った。Firebase の機能である Firebase Authentication を用いて web 上で新規登録、ログインを出来るものを作った。サーバー上でアプリケーションを動かすために AWS の学習・運用を行った。ログイン情報やパスワードやトークンの管理をするための SQL の扱いの学習をした。SQL は PostgreSQL を使い、データベースを構築した。javascript から SQL にアクセスできるようにしてデータベースの管理を行いやすくした。Firebase Authentication のログイン情報を管理し、問題なく運用できるようにした。成果発表ではスライドの作成に携わった。

（文責: 廣井悠真）

4.4 村上光

前期

グループリーダーとして担当教員からの暗号の講義を受ける際、先生とのコミュニケーションや講義後のグループ内でのフィードバックなどを積極的に行った。またグループ内での話し合いではなるべくいろんな人が意見を出せるよう努めた。

サーバサイドの環境を構築するにあたって、サーバについての基礎知識や firebase を使ったメールシステムの機能の開発をメンバーと協力し行った。また使えそうな技術の共有や、仕事の分担などをこまめに相談しながら行った。

中間発表の準備において、Web ページ作成班のグループリーダーと協力しポスターを作った。ポスターを作る際、こまめにプロジェクトメンバーからフィードバックをもらい修正を繰り返し完成させた。

また、夏休み期間にすることの割り振りをグループのメンバーと話し合い計画的に進めることができた。

後期

前期に引き続きグループリーダーとしてグループでの話し合いをまとめたり、積極的に意見を言うことに努めた。スケジュール管理についてはサーバ班で仕事量に応じた日程をメンバーと話し合

いで決め、できなかった際にはまた話し合い、仕事を再分担するという作業を繰り返した。

成果物作成に関してはその人の技術力に合わせた仕事量を相談し分担した。さらにサーバ班内で機能を統合する際、お互いの機能について再確認するため説明し合い、最適な方法で統合することに努めた。また、メール班全体での統合の際には、エラー内容をお互いで確かめ合いトライアンドエラーを繰り返した。

成果物発表会では前期に引き続きポスター作成を Web ページ作成班のグループリーダーと協力して作成した。ポスターは前期と引き続き adobe Illustrator を私用して作成した。作成するうえで、Web ページ班のグループリーダーが adobe Illustrator を使用してポスターを作り、自分が全体のデザインを考えた。また作成したポスターをプロジェクト全体で共有し、メンバーに意見をお願いした。ポスター以外にも成果物発表会での質問予想をメンバーで話し合い、対策を立てたりするなど当日に向けてできることを可能な限り行った。

（文責: 村上光）

4.5 山端祐輝

前期

公開鍵暗号の実装にあたって勉強会や講義など積極的に参加し、理解できるように努めた。勉強をするうえで、疑問点が出てきた場合にはほかのメンバーに質問するなどして疑問点を解消した。また、知識の定着の一環として各々で任意の言語を用いて暗号技術を実装した際には python で elgamal 暗号を実装した。

後期

実際にグループで公開鍵暗号を実装するにあたって、ID ベース暗号を用いたファイルの暗号化を担当することになった。その際に、進捗の報告や連携などを徹底し、わからないところがあれば聞くなど遅れを出さないように意識した。また、プログラム中やスライドの誤植などの訂正などを行い、完成度を高めることができるように努めた。

（文責: 山端祐輝）

第 5 章　結果

5.1　成果

前期の序盤では、教員による暗号化技術に関する講義によって班全体の基礎知識を習得し、また過去の卒業研究生の論文から ID ベース暗号とタイムリリース暗号に関する方式やメリットを理解することで、今後実際にメールシステムにシステムを構築する際に必要となる前提知識を得ることができた。

機能実装の容易さという観点から Google Chrome 拡張機能に対して実装するという決定をした上で、クライアント側とサーバ側でシステムの実装担当のチーム分けを行った。クライアント側では、実際に暗号機能を実装するにあたってプログラムを通して仕組みの理解を深めるために任意の暗号化技術を用いたプログラムの作成を個人で行わせた。サーバ側では、昨年の暗号とセキュリティプロジェクトを参考に、サーバ側の実装における重要なツールの基礎知識を得るために各自必要知識の習得を行わせた。これによって各グループで機能実装にあたって必要な知識をプログラムや実際のツールを通すことで理解を固めることができた。

中間発表では、暗号技術をよく知らない方向けにわかりやすく説明できるような動画・資料作りを行うことや、その上で質疑応答にて、どの部分がわかりづらい資料となっていたのかを明らかにして改めて考えることができた。

後期からは本格的にシステムの実装に入った。メンバーでの話し合いの結果、ID ベース署名と ID ベース暗号を用いたファイルの暗号化とタイムリリース暗号を用いたファイルの暗号化の 3 つの機能を実装するとして活動を始めた。

クライアント側では各メンバーにどの機能を誰が実装するのかを割り当て、まずは Javascript の習得から始め、次に各メンバーでそれぞれ完結した Web ページで各自で担当した暗号が動くようにプログラムの作成を始めた。ここでは作成したプログラムを Google Chrome 拡張に対する実装と同じ状況になるように、本実装と同様に使用する予定であったペアリング暗号化ライブラリである”mcl”と、Javascript を用いて作成することで、今後本実装でもそのまま流用することが可能であるほか、これによって各実装機能についての理解をさらに深めることができたのではないかと考える。

その後、Google Chrome 拡張機能に対する実装を始めた。当初はメール送信時にファイルを添付した際に直接暗号化されたファイルが添付されるようになるシステムを想定していたが、この拡張機能の仕様上この実装が不可能、または難しいことが予測された。このことから代替案をメンバーを話し合った結果、メール送信場所の別の場所にファイルを暗号化出来る部分を用意し、その部分にファイルを添付することで暗号化したファイルをダウンロードでき、そのファイルを添付することで暗号化したファイルを送信することが出来るという案が採用された。このことから、仕様変更を通して有効に問題点を対処する力がついたのではないかと考える。

ファイルの中身すべてを暗号化すると CPU の使用率の増加や動作が重くなるという昨年の暗号とセキュリティプロジェクトの成果から、”crypto-js”という暗号ライブラリを用いて共通鍵暗号方式で暗号化を行った後、その共通鍵を mcl を通した ID ベース暗号またはタイムリリース暗号を用いて暗号化するというハイブリット暗号方式を実装することでこの問題を解決した。

また、ID ベース暗号には送信者と受信者が明確でないとその仕組みが成立しないことから、送信者の認証が可能となる電子署名を機能として加えた。ID ベース署名付きでの送信機能としても電子署名機能はあるのだが、ID ベース暗号に対するファイル暗号化についてもこの機能を加えた。

サーバ側では引き続き必要知識の習得をし、また昨年の暗号とセキュリティプロジェクトを参考にして少しずつ実装を進めていった。ID ベース暗号とタイムリリース暗号ではそれぞれメールアドレスという ID と時間自体が公開鍵となるので、それぞれの通信における秘密鍵を管理するには、鍵生成サーバーが必要であり、その構築を行った。また、ID ベース暗号を用いるためには、利用者の情報をなる ID とそれの認証に必要なパスワードが必要となる。これの管理も必要のため、鍵管理サーバーも必要であり、その構築も同時に行った。認証機能の実装には Firebase を用い、サーバーの実装には Amazon Web Servise を用いることでクライアント側とサーバ側との情報の通信を実現するようにした。

Google Chrome というブラウザに対する実装だけでなく、サーバーとの通信もその処理に含むことから、非同期処理や通信処理に対する理解が必要であったが、署名生成・検証やファイル暗号化・復号を実装することができ、その技術を学習し活用することができた。

（文責: 今井徹雄）

5.2 解決手順と評価

5.2.1 ID ベース署名

ID ベース暗号はその性質上、送信者と受信者を明確にする必要があるため、送信者の認証を行うための ID ベース署名を実装した。メール送信者用とメール受信者用の二つを実装することによって送信者の認証が容易となり、なりすましを防ぐことができるようになったほか、ID ベース暗号の仕組みを確固たるものとした。しかしこれはあくまで本人確認が容易となるものであるため、盗聴などには対応していない。しかしながら、盗聴対策として TLS 通信の使用が対策となり、使用上の問題点はない。

（文責: 山端祐輝）

5.2.2 ID ベース暗号

学内で容易に使える公開鍵暗号として ID ベース暗号を実装した。学内では各々に学生番号が割り振られているため、これを公開鍵として公開鍵暗号を実装することができた。昨年のプロジェクトではファイルの内容をそのまま暗号化すると動作が重くなるという問題を抱えていたため、ファイルの中身を共通鍵暗号で暗号化し、共通鍵を ID ベース暗号で暗号化するというハイブリット暗号方式で実装した。しかし、使用した暗号ライブラリの性質上 txt ファイルのみしか暗号化することができない。そのため、より広い範囲を暗号化できるライブラリを用いるなどしてほかのファイル形式でも暗号化できるようにする必要がある。

（文責: 山端祐輝）

5.2.3 タイムリリース暗号

学内で容易に使える公開鍵暗号の二つ目としてタイムリリース号を実装した。これは時間を公開鍵とするものである ID ベース暗号と同様の理由でファイルの内容をそのまま暗号化するわけにはいかないため、ID ベース暗号と同様にファイルの中身は共通鍵暗号で暗号化し、共通鍵をタイムリリース暗号で暗号化するハイブリッド方式で実装した。しかし、こちらも ID ベース暗号と同様にファイルは txt ファイルのみしか暗号化できないため、ほかのファイル形式でも暗号化できるようにする必要がある。

（文責: 山端祐輝）

5.2.4 Google Chrome 拡張機能における実装

機能実装の容易さという観点を重視した結果、Google Chrome 拡張機能に対する実装を行うことにした。しかし、HTML と Javascript の処理の間に拡張機能を挟み込むことができない仕様の関係上、添付したファイルを拡張プログラム側で受け取り暗号化して添付するという処理を行うことが不可能、または困難であった。そのため、同じ画面の別の場所に暗号化する処理を実行させる部分を加えることでこの問題を解決した。これにより、拡張機能として見た目が不自然にならないようレイアウトの調整等のフロントエンド的な実装項目が増えたが、当初の方針の通りに実装することができた。また、現実的にシステムを構築する際にはこの問題は発生しないため、当初の実装方針通り添付したファイルを直接暗号化することが可能であると考えられる。

（文責: 今井徹雄）

5.2.5 サーバにおける鍵生成処理と鍵の受け渡し

ID ベースの構成における、サーバーでの鍵の受け渡し処理は以下のようになる

1. 送信者は Firebase の認証を用いて、ID とパスワードを入力し、ユーザー情報の登録、ログインを行う。認証には Firebase の機能である、Firebase Authentication を用いた。新規登録、ログインは web サイト上で行えるようにした。新規登録の場合は、メールアドレスとパスワードを登録する画面に移行する。
2. 認証局は JSON Web Token を用いたトークンを返却し、その後、鍵生成局に送られる。
3. AWS のサーバー上に置いたアプリケーションを用いた鍵生成局にトークンが送られる。アプリケーションには GO 言語を使用した。
4. 送られたトークンが本人のものか検証を行う。検証の際 ID やパスワードやトークンの管理には SQL を用いる。今回は PostgreSQL を用いた。
5. 検証結果が問題なければ秘密鍵を送信者に送信する。
6. 送信者は鍵生成局から送られてきた秘密鍵を使い、署名したメールを暗号化したファイルとしてメールサーバーを介して送信される。
7. 受信者は Firebase の認証を用いて、ID とパスワードを入力し、ユーザー情報の登録、ログインを行う。新規登録、ログイン情報は管理者のみが Firebase を通して確認できるようになっている。

8. 認証局は JSON Web Token を用いたトークンを返却し、その後、鍵生成局に送られる。
9. AWS のサーバー上に置いたアプリケーションを用いた鍵生成局にトークンが送られる。
10. 送られたトークンが本人のものか検証を行う。
11. 検証結果が問題なければ公開鍵を受信者に送る。

（文責: 廣井悠真）

第 6 章　各発表会での評価

6.1　中間発表会における評価

中間発表の際に実施した発表評価の集計には、Google Form を使用し 39 件の評価を頂いた。発表技術の評価では、平均で 7.36 であった。発表技術についてのコメントでは、「質問がなくなったときに無言になっている時間が長かったように感じた」、「まとめが弱いように感じた」などの意見が寄せられた。1 つ目のコメントに対する改善点として、発表時間内に何をするのかを事前に決めておくことで無駄な時間を減らすことができると考える。また 2 つ目のコメントについては、後期の成果物発表会では具体的な成果物が完成しているため、まとめの部分もおのずと具体的なものになると考える。

発表内容の評価の平均は 8.00 で発表技術よりも高い評価を頂けた。コメントでは、「暗号化技術についての目標としてしっかり練られたものだと思った」、「知るきっかけになった」などの評価する意見が多く寄せられた。これに関しては初期に行った暗号についての講義や、ポスターや動画作成時にメンバー同士で意見を出し合い改善を繰り返したのが結果につながったと考える。一方で、「しようといている内容はよいと思いましたが、中間発表にしても、作成しようとしているものの具体性が低くて、実際に作成できるのかこころもとなく感じました。」といった意見もあり、これに関してはまだ何を作るかを決めた段階なので、後期の活動を通して具体的な作成手順や手法について考えていく。また、全体的にコメントの内容がメール班よりも Web ページ班のほうが多く書かれていたことからメール班の内容があまり伝わっていないのではないかと推測できる。メール班は暗号という普段身近にないものを短い時間で分かりやすく説明する必要があるので、これに関しては成果物発表会に向けて検討する必要があると考える。

また中間発表会終了後、グループ内で出した反省点として「活動内容に直接関係ない部分が多いので具体的な活動の説明を増やす」、「発表時間内用の簡単な説明を考える必要がある」などが挙げられた。今回、中間発表会を通して得られた意見については成果物発表会で改善していく考えである。

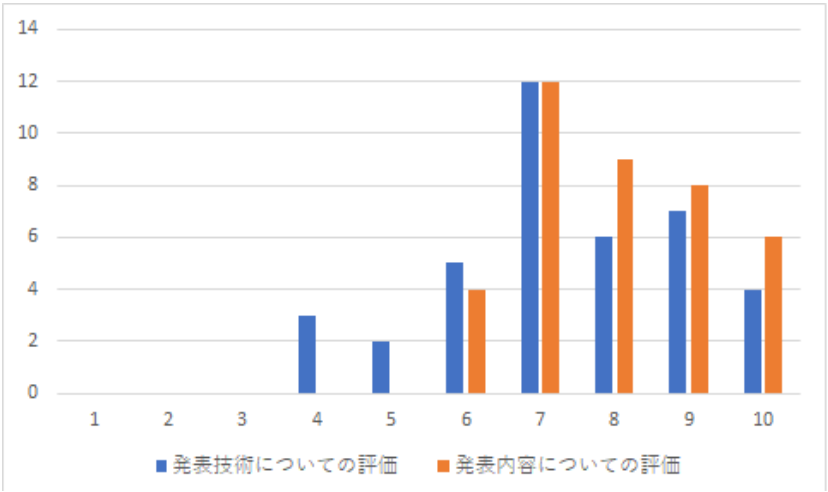

図 6.1　中間発表会アンケート結果

（文責: 村上光）

6.2　成果発表会における評価

発表評価の集計には Google From を使用し 38 件の評価を頂いた。発表技術についての評価では平均 7.45 であった。発表技術についてのコメントでは、「もっと伝えたいことを厳選するか、かみ砕くかしないと初見の言葉が多いため理解しにくかった」、「沈黙が生まれないように工夫して発表している点が良いと思いました」、「質問していくにつれてだんだん理解できた」などの意見が寄せられた。2 つ目のコメントに関しては中間での反省を活かし、事前に何をするかを決めていたことが結果につながったと考える。また 1 つ目と 3 つ目のコメントに関しては、暗号とセキュリティというプロジェクト上、内容が難しく、専門用語が多くなってしまう。さらに、暗号という普段なじみのない言葉が多いので初見でも理解できる工夫を引き続き検討していきたい。

発表内容についての評価の平均は 7.89 と中間に引き続き発表技術よりも高い評価であった。コメントとしては、「プロジェクトやチーム内で作成した目標・目的を達成できるようなものであったと感じました」や、「とても興味深い技術・内容でした。暗号の仕組みにまで踏み込んだ改良などあると良いと思いました。」などの意見のほかに、「全体的に難しくプロジェクトの凄さがあまり伝わってこない」、「タイムリリース暗号のメリットをもっとアピールすれば良いと感じた」などの厳しい意見も寄せられた。やはり内容が難しく、伝わってこないという意見は一定数あり、これに関しては引き続き分かりやすく説明するための工夫は検討すべきだと考える。またタイムリリース暗号のメリットについては、今回は技術の説明よりも成果物の実演のほうを重視したため、タイムリリース暗号についてのメリットが少なく感じられたのではないかと考えられる。しかし全体でみると「興味深い内容だった」、「分かりやすい説明であった」などのコメントが多く、中間発表会での反省点の改善に取り組めたと考える。

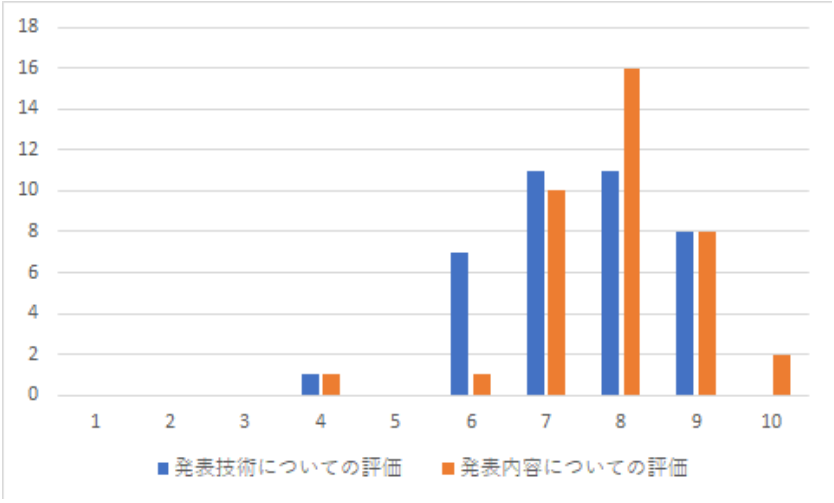

図 6.2　成果発表会アンケート結果

（文責: 村上光）

第 7 章　まとめ

7.1　プロジェクトの成果

チームで一つのシステムを開発することを実際に体験することで、作業の分担やスケジュール管理などチーム開発ならではの経験をすることができた。また成果発表会では、開発したシステムを分かりやすく説明することに尽力し、良い発表をすることができた。

またプロジェクト学習の初期に、暗号の歴史や種類、暗号化・復号の仕組みについて担当教員から講義を受けることでメンバー全員が基本的な知識を身に着けることができた。これは特に、ID ベース暗号とタイムリリース暗号の暗号化・復号のプログラムを担当したクライアント班に活かされていると考えられる。

クライアント班については暗号化･復号の処理についての技術はもちろんだが､他にも JavaScript や Chrome 拡張機能の技術を習得したことにより Web アプリケーションの開発についても身に着けることができた。

またサーバ班では、去年のプログラムを読んだことで http 通信の流れや CORS の設定などサーバについての基本から応用までの知識を身に着けることができた。また、技術面でも firebase や Amazon Web Services、Docker、nginx、SQL などバックエンド開発で用いる技術を習得することができた。

全体的な成果物の成果として、ID ベース暗号とタイムリリース暗号の技術の有用性について確認することができた。これにより、今回のプロジェクトでは公立はこだて未来大学のメールシステムを使い行ったが、仮に新規のメールシステムを実装した際もこの技術は有用であるということが証明された。

（文責: 村上光）

7.2　プロジェクト内の自分の役割

7.2.1　今井徹雄

前期

プロジェクトリーダーの役割として、班ごとの進捗を把握したり、プロジェクト全体での活動を進めたり、方針の決定をする上での進行役を達成できるよう行動した。また、メール班のグループの活動として、教員からの暗号化技術に関する講義が行われた際、率先して振り返りをグループ全体で行うことで班全体の基礎的な知識を身につけることが出来るように貢献したり、クライアント側の活動としてそれぞれ自身で任意の暗号化技術を実装したプログラムを作りそれぞれ共有することで、グループ全体の理解を促すような活動を行った。

また、中間発表会の際は主にポスターや動画のフィードバックを行い、より良い発表になるようこれらの活動に努めた。

後期

成果物に関して主にタイムリリース暗号・Google Chrome 拡張機能への対応・UI の実装・サーバ側との通信を担当した。また、クライアント班の他の方が実装した機能についても、それらのプログラムを統合する際の方式の決定とその管理を行った。Google Chrome 拡張機能に対しては、実際に学内で用いられているメールシステムに対応できるようプログラムを作成し、またその際に UI を調整するといった、主にフロントエンド側の実装を行った。

プロジェクトリーダーの役割としても引き続き班ごとの進捗管理を積極的に行い、また成果発表会におけるポスターや動画といった提出物のフィードバックと改善案の提示も同様に行い、プロジェクトメンバーがより活動しやすくなる活動を行った。

（文責: 今井徹雄）

7.2.2 相馬尚輝

前期

プロジェクト学習で疑問に思った点を確認と共有、学習するためのツールの提案をすることでメンバー間での議論の促進、学習の平滑化を担当した。前期では知識ベースに活動を行ったため、後期ではメンバー間で疑問点や意見を出しやすい環境づくりと学習した技術を制作物を作成するツールへ落とし込む際の理解をメンバー間で深めていけるような役割を果たすことを考えている。

後期

前期に引き続き、疑問に思った点の確認と共有、メンバー間での議論の促進、学習の平滑化を担当した。成果物作成では、メールシステムの ID ベース署名の署名生成と署名検証の部分を担当した。担当箇所は JavaScript, Google Chrome 拡張を使用して作成した。また、作成の際には意見の出し合いにも積極的に参加し、期日までの提出や定期連絡を行うことで班全体としてスムーズに動くために活動できた。

（文責: 相馬尚輝）

7.2.3 廣井悠真

前期

サーバーの環境を構築を担当した。前期はサーバーの利用に関する基礎知識の学習をメインに行なった。利用するシステムの制定を行った。ログイン認証システムは firebase を利用することに決定し、それらの利用方法の施策を行った。ログイン認証システムに利用するプログラミング言語の習得を行った。中間発表はスライドの作成をメインに行なった。

後期

前期に引き続き、学内メールシステムに ID ベース署名・暗号のサーバーの担当を行った。firebase の認証システムを使ったログインシステムの作成を行い、ウェブ上で新規作成・ログイン認証をできるようにした。サーバー上でアプリケーションを動かすために AWS の学習・運用を行った。ログイン情報やパスワードやトークンの管理をするための SQL の扱いの学習をした。

SQL は PostgreSQL を使い、データベースを構築した。javascript から SQL にアクセスできるようにしてデータベースの管理を行いやすくした。成果発表ではスライドの作成に携わった。

（文責: 廣井悠真）

7.2.4 村上光

前期

メール班のグループ活動の際、グループリーダーとして話の進行、スケジュールの管理を行った。また、担当教員からの講義があるときは事前に講義の有無を確認するなど教員とのコミュニケーションを密に行い、他のメンバーに内容を伝えた。

メール班内のサーバ担当として参考資料集めや今後の方針を考え、もう一人のサーバ担当のメンバーと情報を共有した。また、去年のプロジェクト学習の先輩とメールでやり取りを行い、開発手法のヒントなどをもう一人のメンバーと共有した。夏休みに入る前にやるべき仕事を割り振ったり、集まる時間の調整も行った。

中間発表会ではポスター作成を Web ページ作成班のグループリーダーと一緒に担当した。自分はポスター全体のデザインや項目、全体の文章を考えた。また、動画作成班の作った動画について改善案をいくつか提案し、分かりやすいものになるよう行動した。

前期の活動ではグループリーダーとして力不足と感じる場面が多々あったので、後期ではメンバー全員が話しやすい雰囲気を作れるようにしたいと考えている。

後期

グループリーダーの役割として前期に引き続き話し合いをまとめたり、スケジュールの管理や、積極的に意見を言うように努めた。また期末提出物の内容決めや担当の割り振り、LaTeX を使ったグループ報告書の作成を担当した。

成果物作成に関してはサーバ班として Amazon Web Services の設定・運用、クライアントとの通信の SSL 化、nginx を用いたリバースプロキシサーバの作成、去年のコードにタイムリリース暗号の機能を加えた鍵生成局の作成を担当した。また Amazon Web Services のアカウント作成の際には、担当教員と話し合い料金設定を行った。前期に引き続き、去年のプロジェクトの先輩との連絡係を担当し、サーバ班内で出た疑問点などを先輩に質問し、返ってきたものをメンバーと共有した。さらに機能の統合をする際、firebase を使った登録用 Web ページを Amazon Web Services 内で動作できるようにした。またクライアント班にこちらの進捗状況やバグが発生した際のスケジュール調整を積極的に行い、お互いの状況がオープンになるよう努めた。

成果物発表会では前期に引き続き Web ページ班のグループリーダーと一緒にポスター作成を担当した。自分は全体のデザインや文章を考え、見やすいポスターになるよう努めた。その後メンバーからの意見を貰い、その意見に従って作り直すという作業を繰り返した。また、メンバーが作成した動画に関して積極的に意見をするようにし、良いものになるよう行動した。

（文責: 村上光）

7.2.5 山端祐輝

前期

タイムリリース暗号、ID ベース暗号のクライアント側の実装をプロジェクトメンバーと協力して行うためにどこを担当するかなどを話し合った。また、前期の時点では万全に知識を付けられたというわけではなかったため、本格的に実装をはじめることになる後期の活動のためにより暗号への理解を深める必要があると考えていた。ほかにも、中間発表ではスライドをわかりやすくできるよう努力した。

後期

後期では実際にどこを実装するかが決まり、担当は ID ベース暗号を用いファイルを暗号化するプログラムの制作となった。また、そのほかにも成果発表会ではスライドの作成を簡潔にわかりやすくできるように努めたほか、質疑応答にも参加した。

（文責: 山端祐輝）

7.3 今後の課題

- 今回は実装の容易さという観点から Google Chrome の拡張機能を用いて実装したが拡張機能の特性上、メール送信画面にファイルを直接添付した際に直接拡張機能によってファイルを暗号化して、その暗号化したファイルを添付することが難しいことが判明した。しかしこの課題については、新規にメールシステムを構築する際にメールの添付処理自体にこの暗号化処理を施すことで実装することが可能であるため、対処可能であると考える。
- サーバ側の開発において SSL 証明書やドメインを無料のものを使用しているため実用的ではないという問題点がある。有料のものと無料のものを比較してみてもセキュリティ面での強度に違いはないが、有料のもののほうが有効期限やサポートといった観点において優位性があるため、実際に運用する際は有料のものを使用することでより安全にできるのではないかと考える。
- 今回内部動作の実装を目的としているため、ユーザ視点でどのような利点があるのかが分かりづらい。
- 去年のプロジェクト学習に引き続き、Chrome 系ブラウザの開発を行ったが、他のブラウザでの開発もしたいと考える。
- ユーザ登録をする際の Web ページが少し簡易的なものになってしまった。登録するのに必要最低限のことしか書かれておらず、ユーザが安心して行えるような仕様になっていない。

（文責: 村上光）

付録 A　新規習得技術

- ID ベース暗号
- タイムリリース暗号
- firebase
- Amazon Web Services

付録 B　活用した講義

講義名　情報ネットワーク特論 2

活用内容　暗号についての基礎知識を学ぶため担当教員から情報ネットワーク特論 2 の内容の講義を受けた

参考文献

[1] IPA.「2020 年度情報セキュリティに対する意識調査【倫理編】【脅威編】」報告書. IPA 情報処理推進機構. 2021. https://www.ipa.go.jp/security/economics/ishikichousa2020.html , (参照 2022-01-05).

[2] 菅原健斗. タイムリリース暗号を用いた学内向けメールシステムの伴生成. 公立はこだて未来大学卒業論文, 2021.

[3] S/MIME 用証明書 | GMO グローバルサイン【公式】.

[4] Y. Chang and M. Mitzenmacher: Privacy preserving keyword searches on remote encrypted data In: Applied Cryptography and Network Security(ACNS’05), volume 3531 of Lecture Notes in Computer Science, pp.442-455, Springer(2005)

[5] D.Song, D. Wagner and A. Perrig: Practical techniques for searching on encrypted data. In: IEEE Symposium on Research in Security and Privacy, pp.44-55, IEEE (2000) https://jp.globalsign.com/service/clientcert/smime.html , (参照 2022-01-19).

[6] M. Blaze, G Bleumer and M. Strauss: Divertible protocols and atomic proxy cryptography, EUROCRYPT ‘98, 1403, 127-144(1998).