

(単元) 情報安全—安全のための情報技術

(本時のねらい)

共通鍵暗号、公開鍵 (RSA) 暗号、SSL について学び、通信における情報セキュリティの必要性を理解させる。

(ICT 活用方法)

暗号と復号のしくみを説明するために、自作 Excel ソフトを用いて暗号化、復号の体験実習をする。従来は共通鍵暗号については教科書の説明からワークブックでの問題演習を行っていたが、RSA 暗号については計算が非常に煩雑なため紹介するにとどまっていた。ソフトを用いて暗号化、復号を実際にやってみることで理解を深め、共通鍵暗号の利便性と暗号としての強さや RSA 暗号の計算の複雑さを体感する。

(本時の展開)

時間	学習活動	指導事項	I C T活用方法	備考
導入 5分	ID と Pass を入力してログオン。授業の準備をする。	ワークシートを配布。 教材を配布。 本時の目標を説明。	Skymenu より各生徒の PC に Excel 教材を配布する。	
展開 30分	ワークシートで共通鍵暗号の作成と、復号を手作業で行う。 Excel 教材をつかって答え合わせする。 公開鍵暗号の作成と復号を教材を使って体験する。	共通鍵暗号の利便性とその欠点を考えさせる。 公開鍵暗号では暗号化した者でも復号できないことと計算の煩雑さを体験させる。	画面送信機能より、Excel 教材の使い方を説明。 生徒各個人に PC 演習させる。	
まとめ 10分	ワークシートを完成させる。	共通鍵暗号、公開鍵暗号それぞれの長所と短所を考えさせる。	教材回収機能により、演習した Excel 教材を回収し、評価する。	次授業での SSL につなげる。

