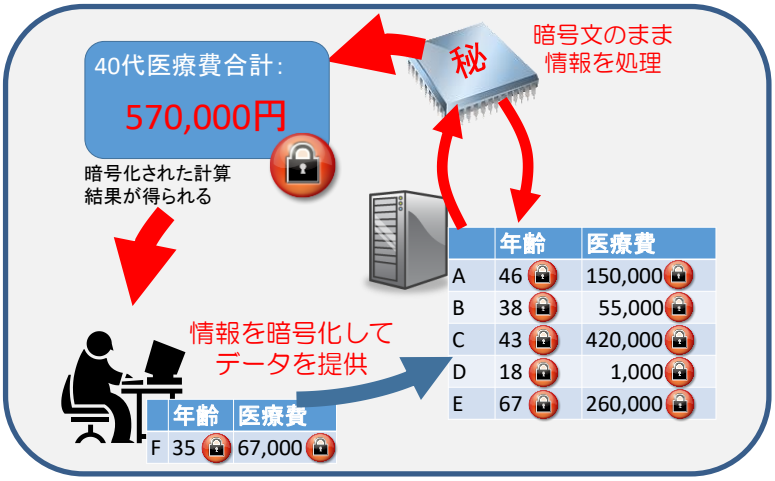
情報科学部　情報セキュリティ研究室

教授　尾花　賢

◆ 研究テーマ

情報セキュリティ研究室では，今日普及が急速に進んできているクラウドコンピューティングを安心安全に利用するための暗号技術の研究を行っています。その中でも特に，秘密分散法や秘匿演算法と呼ばれる暗号技術に取り組んでいます。秘密分散法は，秘密にしたい重要なデータを，複数の部分情報に分散して管理する技術で，一定の個数の部分情報が集まらない限り，元の秘密情報がどのようなデータであったのか全くわからないことを保証する技術です。秘密分散法は，その性質から，重要な情報をクラウドストレージに保存する際などに重要な技術となります。秘匿演算法は，データを暗号化して保存し，そのデータを復号することなく，検索や，統計処理など様々な情報処理を行うことを可能にする暗号技術です。秘匿演算法は，健康情報など，プライバシーに関わる情報を用いてサービスを実現する際に，我々の重要なデータを情報漏洩から守ってくれる鍵となる技術です。



◆ 展示内容

換字暗号と呼ばれる古典的な暗号の解読にチャレンジしましょう！ 換字暗号は下の表のように1文字のアルファベットを別のアルファベットに変換することで暗号化を行う暗号で，例えば，下表のような変換規則を用いるとHELLOという平文は，SHUUXのように暗号化されます。

平文	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	…	Z
暗号文	G	Y	E	P	H	L	A	S	N	C	Z	U	B	R	X	…	T

平文が大文字のアルファベット(26種類)だけからなる場合でも換字暗号の変換規則の数は26!=403291461126605635584000000と膨大な数になるので全ての変換規則を試して暗号解読を行うことは不可能…

しかし，換字暗号は解読可能です！
どうすれば解読できるのでしょうか？チャレンジしてみましょう！