

## 研究タイトル: NP 完全問題の公開鍵暗号への応用 素因数分解アルゴリズムの高速化



氏名:	安細 勉 / ANSAI Tsutomu	E-mail:	ansai@ee.ibaraki-ct.ac.jp
職名:	准教授	学位:	博士(工学)
所属学会・協会:	電子情報通信学会、情報処理学会、応用数理学会		
キーワード:	情報工学、情報セキュリティ		
技術相談 提供可能技術:	<ul style="list-style-type: none"> <li>・情報セキュリティ技術</li> <li>・ネットワーク関連技術</li> <li>・情報処理技術、数値計算関連</li> <li>・コンピュータ 一般</li> </ul>		

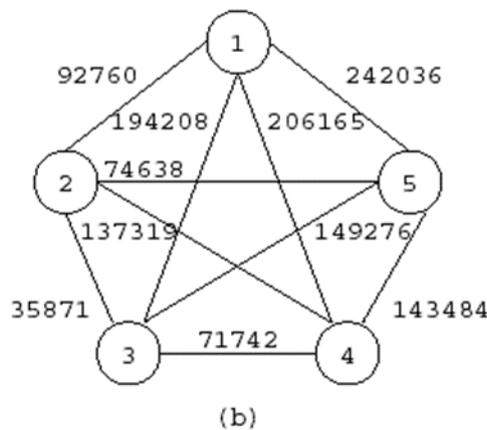
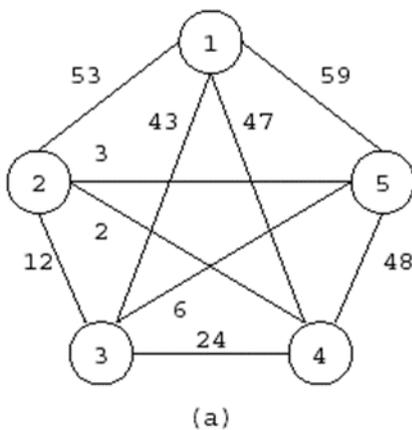
### 研究内容:

#### ・NP 完全問題を用いた公開鍵暗号

暗号とは、他人に知られたくない情報を、第三者に分からないように通信するためのものです。公開鍵暗号は現在ネット上での買い物など、さまざまな場所で利用されている技術で、数学などを使って高速で安全な通信ができるような方法を研究しています。

#### ・電子署名、電子認証技術

これらはハンコやサインのように、本人であることを証明したり、情報が正しい(改ざんされていない)ことを保証する技術です。ネットワーク上での買い物や通信を安心して行なうために重要な技術になっています。



巡回セールスマン問題を  
利用した公開鍵暗号における  
秘密鍵(a)と  
公開鍵(b)の例

### 提供可能な設備・機器:

名称・型番(メーカー)	