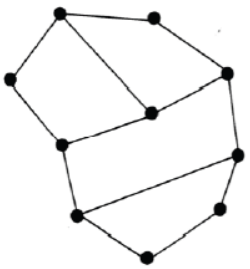
付録R

「こどもあんごう：公開鍵暗号系」の学習（間辺

1. ゲーム「先生に秘密の暗号メッセージ（数）を送ろう」

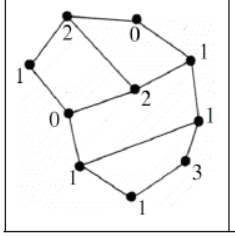
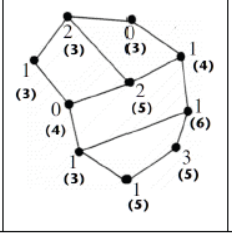
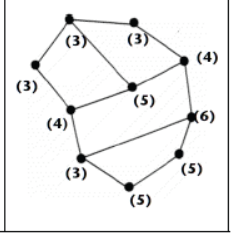
(1) メッセージ表とメッセージ作成用の地図を生徒に配布

（地図は Activity14 で作った地図を使う）

数	メッセージ（例）	地図
10	おなか空いた	
11	眠〜い	
12	授業楽しい！	
・・・		
19	遊びに行きたい	
20	先生、大好き	

(2)「暗号メッセージ」の作り方を説明（数 12 を選んだ場合）

・・・計算ミスをしないように注意させる

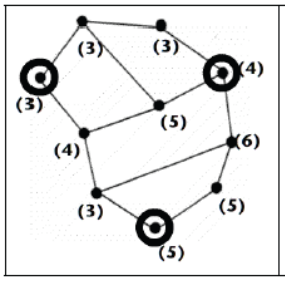
数12を各ノードに振り分ける	それぞれのノードと隣接するノードに振り分けられた数を合計して( )内に書く	( )の数だけを残すこれが「暗号メッセージ」
		

(3) 先生は生徒の作った「暗号メッセージ」を見て次々に解読する

(4)「なぜ先生は解読できたか」を考えさせる

※適宜ヒントを与える：「Activity14 を思い出そう」「アイスクリームバンをどこに置く？」等

(5) 種明かし：先生は解読出来た理由を説明する



・ツーリストタウンで作った地図の親ノードに書かれた数だけを足せば、解読できる

・生徒も自分の作った地図で暗号メッセージを作る／解読することが可能

2. 生徒同士で暗号メッセージを作成し、送受信を行う

3. 先生によるまとめ

- このような地図は「作る事は簡単だけど、解くことは難しい」。
- 複雑なものは地図を公開しても、作った人しか解くことはできない。
- ノードが増えるほど安全性が高くなる。コンピュータを使ってもすぐには解けない。
- この「一方向性」を利用して暗号化通信を行った。
- 地図を公開出来るので、離れた場所にいても暗号化通信が可能になる。
- 「鍵を公開して暗号化通信をする」という原理はインターネットでも使われている。