暗号の数理問題解説 #5

河野

演習問題 2.1

(1) Abel は Briskorn に，公開鍵暗号を利用し，ネットワークを通じて秘密のメッセージを送りたいとする。ただし，ネットワーク上で送られるデータは，常に盗聴者に見られる可能性がある。

次の条件 (a)〜(c) が全て満たされるようにするには，公開鍵暗号を利用して，どのような方法でメッセージを送ればよいか？

(a) Abel が Briskorn に送ったメッセージは暗号化されており，Briskorn 以外の人間は解読できない。

(b) Briskorn は，受け取ったメッセージが確実に Abel が書いたものであり，第 3 者が途中で改ざんしたものではないことを確認できる。

(c) このメッセージを送る過程でそのデータを盗聴した者がいたとしても，その内容を知ることはできない。

注： Abel の公開鍵を P_A，秘密鍵を S_A，Briskorn の公開鍵を P_B，秘密鍵を S_B とする。また，Abel が送るメッセージの平文を T とし，それを，鍵 S_A や P_B などによって暗号化して出来る暗号文を $S_A(T)$, $P_B(T)$ などという記号で表すこと。

(2) A 国と B 国は長年紛争状態にあったが，C 国の秘密調停により和平交渉を行うことになった。A 国と B 国は，この交渉を行うにあたって，多くの秘密文書を通信経路を通してやり取りする必要があるが，これはあくまで秘密交渉の段階であり，A 国，B 国，C 国の交渉担当者以外の者に情報が漏れることを避けなければならない。

A 国から B 国へと秘密文書を送る場合，次の条件 (a)〜(c) が全て満たされるようにするには，公開鍵暗号を利用して，どのような方法で文書のやり取りを行えば良いか？

(a) B 国は，受け取ったメッセージが確実に A 国が作成したものであり，C 国を含めた第 3 者が途中で改ざんした可能性はないことを確認できる。

(b) C 国は，この交渉の過程を把握する必要がある。C 国は，A 国が B 国に送ったメッセージの内容を知る必要があり，さらに，その内容が確実に A 国が B 国に送ったものであることを確認できる。すなわち，A 国が実際に B 国へ送ったものと異なるものを C 国へ送ったり，B 国が実際に A 国から受け取ったものと異なるものを C 国へ送ったり，あるいは，第 3 者が A 国や B 国の名をかたって，A 国から B 国への文書であると偽って C 国へと文書を送ったりすることができないようにする。

(c) これらの文書のやり取りの中で，そのデータを盗聴した者がいたとしても，その内容を知ることはできない。

注 1： ただし C 国は，A 国と B 国の担当者が C 国に無断で勝手にやり取りする文書については，特に確認する方法はないものとする。上の (a)〜(c) は，あくまで A 国が B 国へと文書を送ったという申告があった時に，満たされなければならない条件である。

注 2： A 国の公開鍵を P_A，秘密鍵を S_A，B 国の公開鍵を P_B，秘密鍵を S_B，C 国の公開鍵を P_C，秘密鍵を S_C とする。A 国が B 国へ送ろうとする文書の平文を T とし，それを，鍵 S_A や P_B などによって暗号化して出来る暗号文を $S_A(T)$, $P_B(T)$ などという記号で表すこと。

(3) (2) の A 国と B 国との和平交渉において，A 国は，C 国によって承認された文書を B 国へと送る必要がある場合がある。

次の条件 (a)〜(d) が全て満たされるようにするには，公開鍵暗号を利用して，どのような方法で文書のやり取りを行えば良いか？

(a) B 国は，受け取ったメッセージが確実にA国が作成したものであり，C 国を含めた第 3 者が途中で改ざんした可能性はないことを確認できる。

(b) A 国が B 国へと送る文書は，C 国が一度目を通したものであることを B 国が確認できる。

(c) C 国は，A 国が作成し，C 国が一度目を通した文書が，A 国自身や第 3 者によって改ざんされることなく B 国へと送られたことを確認できる。

(d) これらの文書のやり取りの中で，そのデータを盗聴した者がいたとしても，その内容を知ることはできない。

注： (2) の注 2 と同じ記号を使用すること。

(1) 講義でも解説しましたが書いておきましょう。

送りたいメッセージを T とする。Abel が Briskorn の公開鍵 P_B で T を暗号化して，$P_B(T)$ を送ると，盗聴されていても，盗聴者にそのメッセージは解読できない。しかし，T から $P_B(T)$ を作ることは誰でもできるので，Briskorn はそのメッセージが確かに Abel から来たものかは分からない。すなわち，この状況では問題の条件 (a)，(c) は満足するが (b) を満足しない。

Abel が自分の秘密鍵 S_A で T を暗号化して，$S_A(T)$ を送ると，Briskorn はそのメッセージが Abel からのものであることは分かる。しかし，盗聴者がそのメッセージを盗聴した場合，Abel の公開鍵は公開されているので，その鍵を用いて $P_A(S_A(T)) = T$ となり盗聴者に内容を知られてしまう。すなわち，この状況では問題の条件 (b) は満足するが (a)，(c) を満足しない。

そこで Abel は次のように暗号化を行う。最初に Abel の秘密鍵 P_A で T を暗号化する。このとき $S_A(T)$ が得られる。得られた文書 $S_A(T)$ を Briskorn の公開鍵 P_B で更に暗号化する。得られた文書 $P_B(S_A(T))$ を送る。

この方法が問題の条件 (a)，(b)，(c) を満たしていることを見よう。最終的に P_B で暗号化されているので，この文章を Briskorn 以外が解読することは不可能である。勿論「暗号が破られない」ということを仮定している。よって (a) および (c) は満たされている。Briskorn は S_B を用いて復号化を行い $S_B(P_B(S_A(T))) = S_A(T)$ を得る。更に Abel の公開鍵 P_A を用いて復号化を実行して $P_A(S_A(T)) = T$ を得る。T がきちんとした文章である場合，この文書を送った人間は T から S_A を用いて暗号化したと考えられる。T がきちんとした文章ではなくでたらめの文書の場合は送り手は適当な文書 X を P_A で暗号化し $P_A(X)$ を送った可能性もあるが，きちんとした文章の場合，この可能性はない。よって送り手は Abel の秘密鍵を知っている人物である。Abel の秘密鍵を知っている人物は Abel と考えることができるので，このメッセージは Abel から来たものといえ，条件 (b) も満足する。

(2) A 国は文書 T を自分の秘密鍵 S_A で暗号化し $S_A(T)$ をつくる。それを B 国の公開鍵を用いて更に暗号化し $P_B(S_A(T))$ をつくり B 国に送る。また $S_A(T)$ を C 国の公開鍵を用いて暗号化し

$P_C(S_A(T))$ をつくり C 国に送る。ただし，後で見るように，C 国へ送ることを省略することも可である。

B 国は受け取った $P_B(S_A(T))$ を自分の秘密鍵 S_B を用いて復号化し $S_A(T)$ を得る。次に自分の秘密鍵 S_B を用いて $S_A(T)$ を暗号化し $S_B(S_A(T))$ を得る。更に C 国の公開鍵 P_C を用いて $P_C(S_B(S_A(T)))$ を作り C 国に送る。また $S_A(T)$ を A 国の公開鍵 P_A を用いて復号化し文書 T を得る。

この方法が条件 (a),(b),(c) を満たしていることを見よう。C 国へ送る文書は C 国の公開鍵 P_C で，B 国へ送る文書は B 国の公開鍵 P_B で暗号化されているので，条件 (c) は満たされている。

B 国は自分の秘密鍵で復号化して $S_A(T)$ を得る。これを A 国の公開鍵 P_A で復号化して文書 T を得る。T がきちんとした文章であるということは，送った人間は T を S_A を用いて暗号化したと考えられる。送った人間は A 国の秘密鍵を知っている人間と考えられるので，文書は A 国から来たものであり，改竄されてないと考えられる。よって (a) の条件は満たされる。

まず，A 国が C 国に文書を送らない version を考える。C 国は受け取った文書を自分の秘密鍵で復号化して $S_B(S_A(T))$ を得た後，公開鍵を用いて

$$S_B(S_A(T)) \longrightarrow S_A(T) \longrightarrow T$$

と復号化する。T がきちんとした文章なので，この文章 T は A 国の秘密鍵を知っている人間により暗号化され，その後 B 国の秘密鍵を知っている人間によって更に暗号化されたと見なせる。よってこの文書は A 国で作成され，その後 B 国に送られた文書であることが確認できる。条件 (c) が成り立っていることを確認しよう。B 国が A 国から受け取った文書と異なる文書 T' を偽って C 国に送ろうとしたする。そのためには $S_A(T')$ を作る必要があるが，B 国は A 国の秘密鍵を知らないのでこれは不可能である。この事情は第三者が B 国と偽って C 国に送ろうとする場合も同じである。またこの version では A 国は C 国に文書を送ってないので「異なった文書を送らない」という条件は満たされる。よって条件 (b) も満たされる。

次に A 国が C 国に文書を送る version を考える。この場合 A 国は B 国に送った文書と異なる内容の文書を C 国に送ることは可能である。しかし C 国は B 国から来た文書と照らし合わせることで，その可能性を排除できる。よってこの version も条件を満たす。

2 つの version の違いは B 国が C 国に文書を送らない場合に表れる。送らない version では C 国は B 国がそのようなことをしていることが分からないが，送る version では A 国から文書が来て B 国から来ないという状況になるので，B 国がサボタージュしていることが分かる。ただし A 国が文書を C 国だけに送り，B 国に送らない場合も同様の状況になる。いずれにしろ C 国は「何かおかしな事が起こっている」ことは分かる。

(3) A 国は直接 B 国に文書を送るのではなく，C 国を経由して送ることにする。

A 国は文書 T を自分の秘密鍵 S_A を用いて暗号化する。更に C 国の公開鍵 P_C を用いて $P_C(S_A(T))$ を作成しする。この文書を C 国に送る。

C 国は秘密鍵 S_C を用いて $S_A(T)$ を得ることができる。更に A 国の公開鍵 P_A を用いて $S_A(T)$ を復号化し，T を得る。文書の確認後 C 国は自国の秘密鍵 S_C を用いて文書 $S_A(T)$ を暗号化し，更に B 国の公開鍵 P_B を用いて $P_B(S_C(S_A(T)))$ 作り B 国に送る。

B 国は秘密鍵 S_B を用いて受けとった文書を復号化し $S_C(S_A(T)))$ を得た後，

$$S_C(S_A(T)) \longrightarrow S_A(T) \longrightarrow T$$

と復号化する。前と同様にこの文書は A 国から C 国を経由してきた文書であることが確認できる。

この方法が問題の条件 (a),(b),(c),(d) を満たしていることを見よう。

文書は A 国から C 国へは C 国の公開鍵 P_C で，C 国から B 国へは B 国の公開鍵 P_B で暗号化されたいるので (d) は満たされている。

この文書の最初の暗号化は $T \longrightarrow S_A(T)$ であると考えられる。A 国以外にこのことをできるものはいないので A 国が作成したことが分かる。また S_A を知らないで改竄することはできない。よって (a) は満たされる。

途中 $S_A(T) \longrightarrow S_C(S_A(T))$ という暗号化のプロセスがあるので，この秘密鍵を知っている C 国が目を通していると B 国は確認できる。(b) も満たされる。

文書は $P_B(S_C(S_A(T)))$ なので C 国の秘密鍵を知らない人間が改竄することはできない。また B 国の公開鍵を用いて暗号化されているので，仮りに B 国に届かなかったとしても B 国以外の人間に解読されることはない。確実に届いたことを知りたい場合は届いたという返事を出すという方法もある。どのような返事なら B 国に確実に届いたと C 国が判断できるかを考えてみよ。 よって (c) も確認でき，条件が満たされていることが分かる。

追加演習問題：この解説では C 国を経由して送るとしたが，A 国と C 国であるやりとりの後 A 国から B 国に送るという方法もある。どうやれば実行できるか考えよ。