RFC3766 共通鍵を交換するために使われる公開鍵暗号の強度を判定する

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	この状況における家主は、「2 番目の進入口オプション（玄関の鍵を入れる鍵ボックス）を追加することは、泥棒の仕事を易しくしないようにするために、少なくとも、玄関の鍵と同等の強度であること」を確認しなければなりません。				
	公開鍵暗号技術を使って共通鍵を交換するためにシステムを設計する実装者は、同様な判断をしなければなりません。				
	「どの程度の確信を持って、can この方程式 be used for predicting the difficulty of factoring わずかにより大きな数？」この答えは、「それは、a close upper bound である必要があるが、各素因数分解の労力は、通常、is marked by some improvement in the アルゴリズムs or their 実装s that makes the running time somewhat shorter than the 公式 would indicate」です。				
	それゆえ、セキュアに K bit の鍵を得るためには、実装は、少なくとも、2*K bit をもつ指数を使わなければなりません。				
	Pollard の rho 手法に起因して、the search space in a DH 鍵交換 for the 鍵 (the 指数 in a g^a term),は、その共通鍵の大きさの 2倍大きくなければなりません。				
	「どのようにして、really needed for a discrete logarithm 攻撃 to the number needed to search the keyspace of a cipher コンピュータ命令の数を比較できるのか？」と尋ねられる可能性があります。その労力を計算する際に、「基本演算（basic operation）とは何か？」を考慮する必要があります。				
	理論によって予測された鍵長の推奨事項が、過渡に保守的である可能性があること				
	素朴な想定は、「あなたは、j 回の squarings と j/2 回の multiplies を行う必要があること」				
	あなたが Diffie-Hellman モジュラー指数関数群の大きさを倍にする場合、あなたは、quadruple the number of 演算s needed for the 計算。				
	各演算は、モジュラー reduction を伴わなければならず、それゆえ、その時間の複雑性は、約 16*(.6 + 1) + 1 + 1 ~= 28 n-by-n-word multiplies です。				
	RSA 復号は、that has as many bits as the 法, j指数を使わなければなりません。				
	その計算は、2 回、行われなければならず、各素因数について 1回ずつです。				
	代わりに、人は、TripleDES を破るシステムについて相当する費用と、TripleDES 鍵を防護している公開鍵を破るシステムについて相当する費用を判定しなければなりません。				
	112 bit の攻撃耐性がシステムセキュリティ要件である場合、TripleDES 用の鍵交換システムは、同等の困難性をもつ必要があります。				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	大富豪の攻撃者が、「その専用マシンを共通鍵についてのブルートフォース探索に費やしている」のと同時に、市販の CPU を 112 bit の鍵についての鍵交換を破るために使おうとしている場合、その鍵交換システムは、適切に大きな法を使わなければなりません。				
	「RSA 公開鍵暗号化は、約 2,100 bit の法を使う必要があること」				
	汎用 CPU 攻撃について、あなたは、「約 2400 bit のモジュライは、112 bit の TripleDES 鍵に対する攻撃に対して、概ね同じ強度をもつ」				
	RSA 公開鍵暗号化は、約 2,400 bit の法を使う必要があり、Diffie-Hellman 鍵交換について、人は、顕著な相違点無しに顕著により小さな法を使うことができること				
	「慎重な最低限のセキュリティ要件（ひいては当該鍵交換モジュライ）は、同様の強度をもつ必要があるか？」これに対する答えは、「人が『ムーアの法則』が成立し続けることを期待するか否か？」に依存します。				
	さらなる鍵のビット列を得るためのステップは、下記の要件を充足しなければなりません。: － そのビット列は、鍵交換の秘密について、いかなる情報も明かしてはなりません。 － そのビット列は、相互に相関していてはなりません。 － そのビット列は、鍵交換の秘密についてのすべてのビットに依存しなければなりません 。				
	効率性の観点からは、その共通鍵が巨大な量のエントロピーをもたなければならない場合、おそらく、小さな出力ブロックをもつ暗号技術的ハッシュ関数を使うよりも、大きな出力ブロック（192 bit 以上）をもつものを使うことが最善です。				
	本書中に記述された計算には、乱雑な入力を要求するものがあります。例えば、秘密の Diffie-Hellman 指数は、n の真に乱雑なビット列 （ここで、n は、当該システムのセキュリティ要件)に基づいて選択されなければなりません。				
	当該 DSA モジュールは、DH の法ほどは長くなりませんが、″q″ 部分群の大きさも関係します。				