

	Alice	Bob
Étape 1	Alice et Bob choisissent un nombre premier p et un entier a tel que $1 \leq a \leq p-1$. L'échange n'est pas sécurisé.	
Étape 2	Alice choisit secrètement un nombre x_1 .	Bob choisit secrètement un nombre x_2 .
Étape 3	Alice calcule y_1 tel que : $y_1 \equiv a^{x_1} [p]$.	Bob calcule y_2 tel que : $y_2 \equiv a^{x_2} [p]$.
Étape 4	Alice et Bob s'échangent les valeurs de y_1 et y_2 . L'échange n'est pas sécurisé.	
Étape 5	Alice calcule la clé secrète $y_2^{x_1} [p]$	Bob calcule la clé secrète $y_1^{x_2} [p]$.

1. $y_2^{x_1} \equiv (a^{x_2})^{x_1} [p] \equiv a^{x_2 x_1} [p]$ et $y_1^{x_2} \equiv (a^{x_1})^{x_2} [p] \equiv a^{x_2 x_1} [p]$ d'où $y_2^{x_1} \equiv y_1^{x_2} [p]$.

2. On souhaite appliquer ce protocole avec les clés suivantes :

- clés publiques : $p=81\,629$ et $a=65\,127$.

- clés privées : $x_1=12\,111\,985$ et $x_2=29\,051\,994$.

a) Pour calculer à la main $y_1 \equiv 65\,127^{12\,111\,985} [81\,629]$, on pourrait utiliser la calculatrice en écrivant que $65\,127^2 \equiv 1660$ et en décomposant $12\,111\,985$ en $2 \times 6\,055\,992 + 1$ et en recommençant à chaque fois...

C'est long => plus de 25 étapes :

Handwritten calculation of $65127^{12111985} \pmod{81629}$ using repeated squaring. The steps are as follows:

- $65127 \equiv 65127 \pmod{81629}$
- $65127^2 \equiv 1660 \pmod{81629}$
- $65127^4 \equiv 1660^2 \equiv 27556 \pmod{81629}$
- $65127^8 \equiv 27556^2 \equiv 75816 \pmod{81629}$
- $65127^{16} \equiv 75816^2 \equiv 57117 \pmod{81629}$
- $65127^{32} \equiv 57117^2 \equiv 32717 \pmod{81629}$
- $65127^{64} \equiv 32717^2 \equiv 10717 \pmod{81629}$
- $65127^{128} \equiv 10717^2 \equiv 11517 \pmod{81629}$
- $65127^{256} \equiv 11517^2 \equiv 13117 \pmod{81629}$
- $65127^{512} \equiv 13117^2 \equiv 17117 \pmod{81629}$
- $65127^{1024} \equiv 17117^2 \equiv 29117 \pmod{81629}$
- $65127^{2048} \equiv 29117^2 \equiv 41117 \pmod{81629}$
- $65127^{4096} \equiv 41117^2 \equiv 53117 \pmod{81629}$
- $65127^{8192} \equiv 53117^2 \equiv 65117 \pmod{81629}$
- $65127^{16384} \equiv 65117^2 \equiv 77117 \pmod{81629}$
- $65127^{32768} \equiv 77117^2 \equiv 89117 \pmod{81629}$
- $65127^{65536} \equiv 89117^2 \equiv 11117 \pmod{81629}$
- $65127^{131072} \equiv 11117^2 \equiv 23117 \pmod{81629}$
- $65127^{262144} \equiv 23117^2 \equiv 35117 \pmod{81629}$
- $65127^{524288} \equiv 35117^2 \equiv 47117 \pmod{81629}$
- $65127^{1048576} \equiv 47117^2 \equiv 59117 \pmod{81629}$
- $65127^{2097152} \equiv 59117^2 \equiv 71117 \pmod{81629}$
- $65127^{4194304} \equiv 71117^2 \equiv 83117 \pmod{81629}$
- $65127^{8388608} \equiv 83117^2 \equiv 95117 \pmod{81629}$
- $65127^{16777216} \equiv 95117^2 \equiv 71117 \pmod{81629}$
- $65127^{33554432} \equiv 71117^2 \equiv 59117 \pmod{81629}$
- $65127^{67108864} \equiv 59117^2 \equiv 47117 \pmod{81629}$
- $65127^{134217728} \equiv 47117^2 \equiv 35117 \pmod{81629}$
- $65127^{268435456} \equiv 35117^2 \equiv 23117 \pmod{81629}$
- $65127^{536870912} \equiv 23117^2 \equiv 11117 \pmod{81629}$
- $65127^{1073741824} \equiv 11117^2 \equiv 23117 \pmod{81629}$
- $65127^{2147483648} \equiv 23117^2 \equiv 35117 \pmod{81629}$
- $65127^{4294967296} \equiv 35117^2 \equiv 47117 \pmod{81629}$
- $65127^{8589934592} \equiv 47117^2 \equiv 59117 \pmod{81629}$
- $65127^{17179869184} \equiv 59117^2 \equiv 71117 \pmod{81629}$
- $65127^{34359738368} \equiv 71117^2 \equiv 83117 \pmod{81629}$
- $65127^{68719476736} \equiv 83117^2 \equiv 95117 \pmod{81629}$
- $65127^{137438953472} \equiv 95117^2 \equiv 71117 \pmod{81629}$
- $65127^{274877906944} \equiv 71117^2 \equiv 59117 \pmod{81629}$
- $65127^{549755813888} \equiv 59117^2 \equiv 47117 \pmod{81629}$
- $65127^{1099511627776} \equiv 47117^2 \equiv 35117 \pmod{81629}$
- $65127^{2199023255552} \equiv 35117^2 \equiv 23117 \pmod{81629}$
- $65127^{4398046511104} \equiv 23117^2 \equiv 11117 \pmod{81629}$
- $65127^{8796093022208} \equiv 11117^2 \equiv 23117 \pmod{81629}$
- $65127^{17592186044416} \equiv 23117^2 \equiv 35117 \pmod{81629}$
- $65127^{35184372088832} \equiv 35117^2 \equiv 47117 \pmod{81629}$
- $65127^{70368744177664} \equiv 47117^2 \equiv 59117 \pmod{81629}$
- $65127^{140737488355328} \equiv 59117^2 \equiv 71117 \pmod{81629}$
- $65127^{281474976710656} \equiv 71117^2 \equiv 83117 \pmod{81629}$
- $65127^{562949953421312} \equiv 83117^2 \equiv 95117 \pmod{81629}$
- $65127^{1125899906842624} \equiv 95117^2 \equiv 71117 \pmod{81629}$
- $65127^{2251799813685248} \equiv 71117^2 \equiv 59117 \pmod{81629}$
- $65127^{4503599627370496} \equiv 59117^2 \equiv 47117 \pmod{81629}$
- $65127^{9007199254740992} \equiv 47117^2 \equiv 35117 \pmod{81629}$
- $65127^{18014398509481984} \equiv 35117^2 \equiv 23117 \pmod{81629}$
- $65127^{36028797018963968} \equiv 23117^2 \equiv 11117 \pmod{81629}$
- $65127^{72057594037927936} \equiv 11117^2 \equiv 23117 \pmod{81629}$
- $65127^{144115188075855872} \equiv 23117^2 \equiv 35117 \pmod{81629}$
- $65127^{288230376151711744} \equiv 35117^2 \equiv 47117 \pmod{81629}$
- $65127^{576460752303423488} \equiv 47117^2 \equiv 59117 \pmod{81629}$
- $65127^{1152921504606846976} \equiv 59117^2 \equiv 71117 \pmod{81629}$
- $65127^{2305843009213693952} \equiv 71117^2 \equiv 83117 \pmod{81629}$
- $65127^{4611686018427387904} \equiv 83117^2 \equiv 95117 \pmod{81629}$
- $65127^{9223372036854775808} \equiv 95117^2 \equiv 71117 \pmod{81629}$
- $65127^{18446744073709551616} \equiv 71117^2 \equiv 59117 \pmod{81629}$
- $65127^{36893488147419103232} \equiv 59117^2 \equiv 47117 \pmod{81629}$
- $65127^{73786976294838206464} \equiv 47117^2 \equiv 35117 \pmod{81629}$
- $65127^{147573952589676412928} \equiv 35117^2 \equiv 23117 \pmod{81629}$
- $65127^{295147905179352825856} \equiv 23117^2 \equiv 11117 \pmod{81629}$
- $65127^{590295810358705651712} \equiv 11117^2 \equiv 23117 \pmod{81629}$
- $65127^{1180591620717411303424} \equiv 23117^2 \equiv 35117 \pmod{81629}$
- $65127^{2361183241434822606848} \equiv 35117^2 \equiv 47117 \pmod{81629}$
- $65127^{4722366482869645213696} \equiv 47117^2 \equiv 59117 \pmod{81629}$
- $65127^{9444732965739290427392} \equiv 59117^2 \equiv 71117 \pmod{81629}$
- $65127^{18889465931478580854784} \equiv 71117^2 \equiv 83117 \pmod{81629}$
- $65127^{37778931862957161709568} \equiv 83117^2 \equiv 95117 \pmod{81629}$
- $65127^{75557863725914323419136} \equiv 95117^2 \equiv 71117 \pmod{81629}$
- $65127^{151115727451828646838272} \equiv 71117^2 \equiv 59117 \pmod{81629}$
- $65127^{302231454903657293676544} \equiv 59117^2 \equiv 47117 \pmod{81629}$
- $65127^{604462909807314587353088} \equiv 47117^2 \equiv 35117 \pmod{81629}$
- $65127^{1208925819614629174706176} \equiv 35117^2 \equiv 23117 \pmod{81629}$
- $65127^{2417851639229258349412352} \equiv 23117^2 \equiv 11117 \pmod{81629}$
- $65127^{4835703278458516698824704} \equiv 11117^2 \equiv 23117 \pmod{81629}$
- $65127^{9671406556917033397649408} \equiv 23117^2 \equiv 35117 \pmod{81629}$
- $65127^{19342813113834066795298816} \equiv 35117^2 \equiv 47117 \pmod{81629}$
- $65127^{38685626227668133590597632} \equiv 47117^2 \equiv 59117 \pmod{81629}$
- $65127^{77371252455336267181195264} \equiv 59117^2 \equiv 71117 \pmod{81629}$
- $65127^{154742504910672534362390528} \equiv 71117^2 \equiv 83117 \pmod{81629}$
- $65127^{309485009821345068724781056} \equiv 83117^2 \equiv 95117 \pmod{81629}$
- $65127^{618970019642690137449562112} \equiv 95117^2 \equiv 71117 \pmod{81629}$
- $65127^{1237940039285380274899124224} \equiv 71117^2 \equiv 59117 \pmod{81629}$
- $65127^{2475880078570760549798248448} \equiv 59117^2 \equiv 47117 \pmod{81629}$
- $65127^{4951760157141521099596496896} \equiv 47117^2 \equiv 35117 \pmod{81629}$
- $65127^{9903520314283042199193993792} \equiv 35117^2 \equiv 23117 \pmod{81629}$
- $65127^{19807040628566084398387987584} \equiv 23117^2 \equiv 11117 \pmod{81629}$
- $65127^{39614081257132168796775975168} \equiv 11117^2 \equiv 23117 \pmod{81629}$
- $65127^{79228162514264337593551950336} \equiv 23117^2 \equiv 35117 \pmod{81629}$
- $65127^{158456325028528675187103900672} \equiv 35117^2 \equiv 47117 \pmod{81629}$
- $65127^{316912650057057350374207801344} \equiv 47117^2 \equiv 59117 \pmod{81629}$
- $65127^{633825300114114700748415602688} \equiv 59117^2 \equiv 71117 \pmod{81629}$
- $65127^{1267650600228229401496831205376} \equiv 71117^2 \equiv 83117 \pmod{81629}$
- $65127^{2535301200456458802993662410752} \equiv 83117^2 \equiv 95117 \pmod{81629}$
- $65127^{5070602400912917605987324821504} \equiv 95117^2 \equiv 71117 \pmod{81629}$
- $65127^{10141204801825835211974649643008} \equiv 71117^2 \equiv 59117 \pmod{81629}$
- $65127^{20282409603651670423949299286016} \equiv 59117^2 \equiv 47117 \pmod{81629}$
- $65127^{40564819207303340847898598572032} \equiv 47117^2 \equiv 35117 \pmod{81629}$
- $65127^{81129638414606681695797197144064} \equiv 35117^2 \equiv 23117 \pmod{81629}$
- $65127^{162259276829213363391594394288128} \equiv 23117^2 \equiv 11117 \pmod{81629}$
- $65127^{324518553658426726783188788576256} \equiv 11117^2 \equiv 23117 \pmod{81629}$
- $65127^{649037107316853453566377577152512} \equiv 23117^2 \equiv 35117 \pmod{81629}$
- $65127^{1298074214633706907132755154305024} \equiv 35117^2 \equiv 47117 \pmod{81629}$
- $65127^{2596148429267413814265510308610048} \equiv 47117^2 \equiv 59117 \pmod{81629}$
- $65127^{5192296858534827628531020617220096} \equiv 59117^2 \equiv 71117 \pmod{81629}$
- $65127^{10384593717069655257062041234440192} \equiv 71117^2 \equiv 83117 \pmod{81629}$
- $65127^{20769187434139310514124082468880384} \equiv 83117^2 \equiv 95117 \pmod{81629}$
- $65127^{41538374868278621028248164937760768} \equiv 95117^2 \equiv 71117 \pmod{81629}$
- $65127^{83076749736557242056496329875521536} \equiv 71117^2 \equiv 59117 \pmod{81629}$
- $65127^{166153499473114484112992659751043072} \equiv 59117^2 \equiv 47117 \pmod{81629}$
- $65127^{332306998946228968225985319502086144} \equiv 47117^2 \equiv 35117 \pmod{81629}$
- $65127^{664613997892457936451970639004172288} \equiv 35117^2 \equiv 23117 \pmod{81629}$
- $65127^{1329227995784915872903941278008344576} \equiv 23117^2 \equiv 11117 \pmod{81629}$
- $65127^{2658455991569831745807882556016689152} \equiv 11117^2 \equiv 23117 \pmod{81629}$
- $65127^{5316911983139663491615765112033378304} \equiv 23117^2 \equiv 35117 \pmod{81629}$
- $65127^{10633823966279326983231530224066756608} \equiv 35117^2 \equiv 47117 \pmod{81629}$
- $65127^{21267647932558653966463060448133513213216} \equiv 47117^2 \equiv 59117 \pmod{81629}$
- $65127^{42535295865117307932926120896267026426432} \equiv 59117^2 \equiv 71117 \pmod{81629}$
- $65127^{85070591730234615865852241792534052852864} \equiv 71117^2 \equiv 83117 \pmod{81629}$
- $65127^{17014118346046923173170448358506810505728} \equiv 83117^2 \equiv 95117 \pmod{81629}$
- $65127^{34028236692093846346340896717013621011456} \equiv 95117^2 \equiv 71117 \pmod{81629}$
- $65127^{68056473384187692692681793434027242022912} \equiv 71117^2 \equiv 59117 \pmod{81629}$
- $65127^{136112946768375385385363586868054484045824} \equiv 59117^2 \equiv 47117 \pmod{81629}$
- $65127^{272225893536750770770727173736108968091648} \equiv 47117^2 \equiv 35117 \pmod{81629}$
- $65127^{544451787073501541541454347472217936183296} \equiv 35117^2 \equiv 23117 \pmod{81629}$
- $65127^{1088903574147003083082908694944435872366592} \equiv 23117^2 \equiv 11117 \pmod{81629}$
- $65127^{2177807148294006166165817389888871752733184} \equiv 11117^2 \equiv 23117 \pmod{81629}$
- $65127^{4355614296588012332331634779777743505466368} \equiv 23117^2 \equiv 35117 \pmod{81629}$
- $65127^{8711228593176024664663269559555487010932736} \equiv 35117^2 \equiv 47117 \pmod{81629}$
- $65127^{17422457186352049329326539119109740218665472} \equiv 47117^2 \equiv 59117 \pmod{81629}$
- $65127^{34844914372704098658653078238219480437330944} \equiv 59117^2 \equiv 71117 \pmod{81629}$
- $65127^{69689828745408197317306156476438960874661888} \equiv 71117^2 \equiv 83117 \pmod{81629}$
- $65127^{139379657490816394634612312952877921749323776} \equiv 83117^2 \equiv 95117 \pmod{81629}$
- $65127^{278759314981632789269224625905755843498647552} \equiv 95117^2 \equiv 71117 \pmod{81629}$
- $65127^{55751862996326557853844925181151168699729504} \equiv 71117^2 \equiv 59117 \pmod{81629}$
- $65127^{11150372599265311570768985236230233739945008} \equiv 59117^2 \equiv 47117 \pmod{81629}$
- $65127^{22300745198530623141537970472460467479890016} \equiv 47117^2 \equiv 35117 \pmod{81629}$
- $65127^{44601490377061246283075940944920934959780032} \equiv 35117^2 \equiv 23117 \pmod{81629}$
- $65127^{89202980754122492566151881889841869959560064} \equiv 23117^2 \equiv 11117 \pmod{81629}$
- $65127^{178405961508244985132303763779683739919120128} \equiv 11117^2 \equiv 23117 \pmod{81629}$
- $65127^{356811923016489970264607527559367479838240256} \equiv 23117^2 \equiv 35117 \pmod{81629}$
- $65127^{713623846032979940529215055118734959676480512} \equiv 35117^2 \equiv 47117 \pmod{81629}$
- $65127^{1427247692065959881058430110237469919352961024} \equiv 47117^2 \equiv 59117 \pmod{81629}$
- $65127^{2854495384131919762116860220474939838705922048} \equiv 59117^2 \equiv 71117 \pmod{81629}$
- $65127^{5708990768263839524233720440949879677411844096} \equiv 71117^2 \equiv 83117 \pmod{81629}$
- $65127^{11417981536527679048467440881899759354223688192} \equiv 83117^2 \equiv 95117 \pmod{81629}$
- $65127^{22835963073055358096934881763799518708447376384} \equiv 95117^2 \equiv 71117 \pmod{81629}$
- $65127^{45671926146110716193869763527599037416894752768} \equiv 71117^2 \equiv 59117 \pmod{81629}$
- $65127^{91343852292221432387739527055198074833789505536} \equiv 59117^2 \equiv 47117 \pmod{81629}$
- $65127^{182687704584442864775479054110396149667579011072} \equiv 47117^2 \equiv 35117 \pmod{81629}$
- $65127^{365375409168885729550958108220792299335158022144} \equiv 35117^2 \equiv 23117 \pmod{81629}$
- $65127^{730750818337771459101916216441584598670316044288} \equiv 23117^2 \equiv 11117 \pmod{81629}$
- $65127^{1461501636675542918203832432883169197340632088576} \equiv 11117^2 \equiv 23117 \pmod{81629}$
- $65127^{292300327335108583640766486576633839468126417$