Sending Secrets: Cryptography and Privacy in a Quantum World

Cristopher Moore Santa Fe Institute

Harpers, issue 179, June/November 1939



Is it not a curious fact that in a world steeped in irrational hatreds which threaten civilization itself, men and women—old and young—detach themselves wholly or partly from the angry current of daily life to devote themselves to the cultivation of beauty, to the extension of knowledge, to the cure of disease, to the amelioration of suffering, just as though fanatics were not simultaneously engaged in spreading pain, ugliness, and suffering?

Writing

11111 WII WA 1.1. 81 1.1:+1=1= =1 =12 21 11- 100 0, 0, ... X11041 222.9 11 W T T T 死 美山豆 mi 2 - 12 - 12 L'ant

12

目

RA.

Secret writing



bedefghl G 1 B 9 C Z J I m n o p q X b * 9 5, 9 2 cr ett. St 97 937. r 4

Secret writing



The Code alphabet a a or g n m & n 1 t m n b l h Z e 2 UÚ to, too, two 0 ⊿ p 3 the, three V e hkqq for, four 4 W t I wr x x and





Shift each letter three places in the alphabet:





Shift each letter three places in the alphabet:





Plaintext: ET TU BRUTE

Shift each letter three places in the alphabet:





Plaintext: ET TU BRUTE

Ciphertext: HW WX EUXWH

Shift each letter three places in the alphabet:





Plaintext: ET TU BRUTE

Ciphertext: HW WX EUXWH

To decode, just shift backwards

Shift each letter three places in the alphabet:





Ciphertext: HW WX EUXWH

To decode, just shift backwards

26 possibilities







The Kama Sutra recommends that women learn the art of secret writing, to help them conceal their liaisons



The Kama Sutra recommends that women learn the art of secret writing, to help them conceal their liaisons





The Kama Sutra recommends that women learn the art of secret writing, to help them conceal their liaisons



Plaintext: MEET ME BY THE BANYAN TREE



The Kama Sutra recommends that women learn the art of secret writing, to help them conceal their liaisons



Plaintext: MEET ME BY THE BANYAN TREE

Ciphertext: AHHL AH TK LBH TZSWZS LGHH



The Kama Sutra recommends that women learn the art of secret writing, to help them conceal their liaisons



Plaintext: MEET ME BY THE BANYAN TREE

Ciphertext: AHHL AH TK LBH TZSWZS LGHH

To decode, look up the letters in the scrambled alphabet



The Kama Sutra recommends that women learn the art of secret writing, to help them conceal their liaisons



Plaintext: MEET ME BY THE BANYAN TREE

Ciphertext: AHHL AH TK LBH TZSWZS LGHH

To decode, look up the letters in the scrambled alphabet

26×25×24...3×2×1 = 403,291,461,126,605,635,584,000,000 possibilities



دا سمالده ما دواليم وبصف والكلومالغن واحرة مره المالي مروم مرماليرلد مر ما عاد الد معاد سعد مقد الم منطق من المحلي منا معال اللمر وسحت ولا ال د ما مسلما والمعرو واحداد والحوم الا مع مع معالما منسب وعال وسعاد و معد ما معد المراد و الما معد المعل والمد والمد والمعالية وسعاد و مع مراكرها، للرداد و الما ماراميخ دكره والد والرك والمعال السر والمراسية مع مراكرها، للرداد و الما ماراميخ دكره والد والرك والمعال السر والما العيادة المع مع مراكرها، للرداد و الما ماراميخ دكره والد والرك والمعال السر والمراسية مع مراكرها، للرداد و الما ماراميخ دكره والد والرك والمعا السر ماليا، العيادة الم مع مراكرها، للرداد و والم الماح دكره والد والرك والمعا السر ماليا، العيادة الم مع مراكرها، للرداد و والم الماح دكره والد والمع وحمة والم المراحية و والما المعاد والم معر مراكرها، والم ما والج إلمرما وعسل الطرر بالصدر المار الما من م

مراادا - والحداله رد العالم وطراب علم مدمر والب ج

لسمالد المحسب مراكر مع المرحم ومسالله وحسمالد وجدم وسالد الاست معود ملحوالد وعاسلهم العرع لالالعاس لهذه معالد فلم ليدة علما مارزي مع وكام الودر الحدل الاستولع مارس الكرالعساد ولصلي للتوجر مزامنون فالولد الارسي سالا والمنام الغول عفال الدارد لولاح المراذ ومناطق والنا محسر الوويو وسادد المنام الغول المامالد وسعول واداد بناويوهمان ولعرد الما العرق والما المحالمة

The most common letters are E, T, A, O, I, N

دا سمالده ما دالدم ومحمد والكلوم العنتي اعدة مرد الإلكان مروعهم مالد عرف مد ما عام الد معار سمع معلوا في خطو للمحرية المعلي منا عواللم وسحد ولا بلا ما ما مسلم المعلول ويلحون والمعلوم الموضح معلما منسى وعالو وسحل و ما محر سعيد سرد علما لعد الملي ورو المع مع والمراسل المحرو إسعا م مراكحه المرباد والما والمرح وكر والمنه والرك والمعالية السالة السالة الا مد مراكحه المرباد والما والمرح وكر والمنه والرك والمع الس الما العبالة الا مد مراكحه المرباد والما والمرح وكر والمنه والرك والمع الس والما العبالة الد مد مراكحه المرباد والما والمرح وكر والمنه والرك والمع الس والما العبالة الد مد مراكحه المرباد والما والمرح وكر والمنه والرك والمع الس والما العبالة العباد مد مراكحه المرباد والما والمرح والمنه والمرك والمع وحنه والم المرا العباد والمرابس مد مراكحه المرباد والما والم

فراادلد والجداله ودالعالم وطراب علم مدمج والسه

لسمايد الحسب مراجع مراجع مع المحسم وحسمايد وجدم وساد الاست يعور ملحوالدور المعرام العرع الالاصل محد معاند مما يدفر علما مرت سمه وكات الوديد الحدل الاستولم مارس الكرالعساد ولاصلي الدور مرافعان فالحراد الارسي السياد والمنام المعمول عقاد الدار والدر المتع المراذ ومن النول ولام والما المعرون والمنام العول المامعاد وستول واداد المناويون الدولي والما العظر الما المعوال

The most common letters are E, T, A, O, I, N

Doubled letters: LL, EE, SS, OO

دا سمالده ما دالدم ومحمد والكلوم المنتواحدة مره المال مراجع ما العرار مد ما عاد الدم ويحد بقد في منطق من المراجع ويتا معلم ما عواللم وسحد ولا المر د ما مسلم المراجع ويلحون والمنطق الا في محمد الما مسي وعالو وسحله و ما محر سيد مرد علما لعد الملي والم الا في معالم الميا معالي وسعله و مد مراكرها، لمرياد والما والمرح وكر والمنه والرك والمع السي المراد العيادة الدم مد مراكرها، لمرياد والما والمرح وكر والمنه والرك والمع السي المراد العيادة المرابع مد مراكرها، لمرياد والما والمرح وكر والمنه والرك والمع السي المراد العيادة المرابع مد مراكرها، لمرياد والما والمرح وكر والمنه والرك والمع السي المراد العيادة الدم مد مراكرها، لمرياد والما والمرح وكر والمنه والرك والمع السي والما العيادة الدم مد مراكرها، لمرياد والما والمرج وكر والمنه والرك والمع السي الما العيادة الدم مد مراكرها، ويد الما والم والم والماء والما والما والما والم والما المي والما العياد والم

فراادا - والحداله رد العالم ومطرا الدعلم مدمجة والسدم

لسمالد المحسب المرحسم ومسلم ومسلم العربي ومسلما للعربي ومسلما للعربي ومسلما للعربي ومسلما للعربي ومسلم العربي ومسلم المعربي المحاسر ومسلم المعربي المحاسر ومسلم ومسلم

The most common letters are E, T, A, O, I, N

Doubled letters: LL, EE, SS, OO

Digrams: letter pairs like QU that go together

ذا سمالده ما داليم مصف والكلوم العنتوا عرد مرد المالي مراجع ما ليرا مر ما عام الد معام سمع منعوا في منطق لمرينا معلم ما عواللم وسحد ولا ملا ما ما معام الد معام معاد والحوم الور فع مصللاً مسيح وعلو به وسعله و ما حر سيد مرد علما لعد العلي مع الور فع مصللاً مسيح وعلو به وسعله و ما حر سيد مراجعاً له ما لعد العلي مع ولا معام المراسي للروا اسعار مراجعاً لم باد والداد المرح وكر والما و والرك وله ما السر ماليا، العبادة الا مسم والسفام المراجع المراجع ولي والمحمد والرك وله مراجعاً والالاليم و بع اسم والسفام المراجة إلم ما وعسل القرر ما العد والرك المعاد م

فراادلد والحداله ردائعالم ومطرا لاعام مدمجة والسدج

لسمالد المحسب والرحسم وسالد الاست معود والمحواليور واسترام المعرع لالالعاس محد معالد مما ودفر علما مرت سمه وكان الودر الحدل الاستراح مارس التدليع ماه ولتصار للدو ورم النول فالوله الارسر السراسيا لارالمنام المعول عناد الراسال لي المحمد المراذ ومن النول فالوله الارسر الوقو وسرد المنام العول عناد الراستول وارالوناو موالما: ولتر والما العتم والمول الما السيوالي

The most common letters are E, T, A, O, I, N

Doubled letters: LL, EE, SS, OO

Digrams: letter pairs like QU that go together

Punctuation and spaces help a lot

دا سمالده ما دالدم ومحمد والكلوم العنتي اعدة مرد الإلكان مروام مرما العرف مد ما عام الد معام سمع مقع في منطق مرينا معلم ما عوالله وسخل وللما م ما مع عام الد معام سمع مقع في منطق من معام معلي مناطع وسخل و ما مع منه ما المعالي والحرول والمع مع والديل الميا مع والروسل للمود إسعا م مراكزها المرداد والداد المريخ وكرد والمد والرك والمعالية الس الما العيادة الديس م مراكزها المرداد والداد المريخ وكرد والمد والرك والمع الس الما العيادة الديس م مراكزها المرداد والما والمريخ وكرد والمد والرك والمع الس الما العيادة الديس م مراكزها المرداد والمراج وكرد والمد والرك والمعار الس الما العيادة الديس م مراكزها المرداد والما والمريخ وكرد والمد والرك والمعام الس والمراجع والمريس م مراكزها والمرد والمراجع وكرد والمد والمريخ وكرد والما مراكسان والما لمراجع و م مراكزها والمراجع والمراجع والمود والمريخ وكرد والما والمراجع والمريس

فرااداد والحداله ودالعالم ومطرا الدعام مدمج والسدج

لسمايد المحسب مراكر حسم وسالد الاست معدم الرحسم المعذمة الاست الاست معدم المعرب العرب العربي المعربي الواعس المدارع مال وفر علما مرت سم وكان الموديد الحمل الاستولي مارس المدارع ما ولت وفر علما مرت سم وكان أموديد الدرسيل سالا والمنام المعول المالية اسراد بواطل والموالية ومرة النول والمراسية والمعالية المعول المامعاد وسعول ودر الدناو موالما: ولحم والما العظم الما السعالة

The most common letters are E, T, A, O, I, N

Doubled letters: LL, EE, SS, OO

Digrams: letter pairs like QU that go together

Punctuation and spaces help a lot

ذا سمالده ما دالدم و بحد من طلام المعند احدة مرد المال المربع مرادعرا. مر ما عام اله معام سعد ميسواف سلم مح بنا معلم ما عواللم و سحد طلاما م ما د مسلم المراحية و الحواف سلم و بنا معلم منا معلم منا على المعر و المعلم و ما د مسلم المراحية و الحواف المربع و المراحية معالم مسحد و عالم به و سعلم و ما حر معجود مرد علما المعد الملي مع و المراحية و الروسية المحرور المعلى م مراكم ما المراح و الداد المربح و كل و المد و المراحية و المراحية المعادة المعادة و معر مراكم ما المراح و الداد المربح و كل و المد و المراحية و المراحية المعادة المعادة المعادة المراحية م مراكم ما المراحية و الداد المربح و كل و المد و الركم و المراحية المراحية و المراحية م مراكم ما المراحية و الداد المربح و كل و المد و المركم و المعاد و المراحية المراحة و المراحية و معر مراكم المراحة و المراحية و المرحة و المعلم و حدة و المراحية و و المراحية و المراحية و المراحية و المراحية و محسم مراكم المراحة و المراحة و المحمة و المعلم و حدة و المراحية و الما المعادة المراحة و المراحية و المحمة و الم

مراادلد والعداله ردالعالم ومطرا الدعلم مدعد والسدج

لسمايد المحسب مراكر حسم وسالد الاست يعور ملحوالدي استرام المعرع للالعاس محمد معاند مما ودفر علما مرت سم وكان الوديد الحسل الاسترام مارس التداريساد وممار الدور من الغول فالوله الارسير المساد والمنام المعول عنهاد الراسلول معلوات والفران فالوله الارسير اليوبيو وسريد الفاد العول المامغان وسيعول واداد المناويون الدولي والما العرق والما المحالي

Al-Kindi, 801-873

JNN YBMF NK R HNNW JFQXH QU INXWDEKBG

The most common letters are E, T, A, O, I, N

Doubled letters: LL, EE, SS, OO

Digrams: letter pairs like QU that go together

Punctuation and spaces help a lot

الدادار والعدائه والعالم ومرالعا لمروط الدعلم مدمج والسدج

لسمالد المحسب والرحسم وسالد الاست ومعرب المحسم ومسلح المعرع للالعاس محد معالد مما ودخ علما مرت سمه وكان الوديد الحدل الاستولج مارس الكرالعساد ولتصار الدو ورم الغنان فالولد الارس السيالا المنام الغلول عنادالا اسلاد والعمار الدومة الغنان فالولد الارس السيالا المنام الغلول عنادالا اسلاد وسعول واراد المناو موالما النحس الدوس وسلا المنام الغلول

Al-Kindi, 801-873

JNN YBMF NK R HNNW JFQXH QU INXWDEKBG JOO YBMF OK R HOOW JFQXH QU IOXWDEKBG

The most common letters are E, T, A, O, I, N

Doubled letters: LL, EE, SS, OO

Digrams: letter pairs like QU that go together

Punctuation and spaces help a lot

دا معالده ما داليم وبصف والكلوم العنتي اعرة مرد الكال مريم مراسع له مر ما علم الد معاد سعد منه والع منطولي بنا معلم منا عواللم وسعد ولا بلا د ما معام الد معاد معاد والعراق منطولي من معلم منا عمال معنى ولا بلا ما مع منه معروب مرد علما لعد العلي مرابع مع والرو معاد معاد معاد وسعلم و معر مراكرها كرباد والداد المرح وكر والم والرو والمعاد والروسل للمروا بعلى مسم مراكرها والمراج وكر والم والمع وحن والم مرابعا والمرابع العمادة المرابع مسم مراكرها والم والمراج وكر والم والمرو والمع وحن والم مرابعا والمرابع والروسل المروم والمحال

فراادله _ والحداله رد العالم ومطرا بدعام مدمج والد مع

لسمالد المحسب والرحسم وسالد الاست معود والمحواليور واسترام المعرع لالالعاس محد معالد مما ودخ علما مرت سمه وكان الودر الحدل الاستراح مارس الكراليع الد والتصار المقوم والغول فالولد الارسير المسالا والمنام الفعول عنها والا اسراد و المراق مع الغراق والمن النه مراليوس وسرد الفاد العام المامعاد وسعول وادادينا وجوهما: ولحروا الاالعظم والمسالا والمناو الغ

JNN	YBMF	NK	R	HNNW	JFQXH	QU	INXWDEKBG
J00	YBMF	OK	R	$\mathrm{H}\mathbf{O}\mathbf{O}\mathbb{W}$	JFQXH	QU	IOXWDEKBG
TOO	YBMF	OK	R	HOOW	T FQXH	QU	IOXWDEKBG

The most common letters are E, T, A, O, I, N

Doubled letters: LL, EE, SS, OO

Digrams: letter pairs like QU that go together

Punctuation and spaces help a lot

دا معالده ما داليم وبصف والكلوم العنتي اعرة مرد الكال مريم مراسع له مر ما علم الد معاد سعد منه والع منطولي بنا معلم منا عواللم وسعد ولا بلا د ما معام الد معاد معاد والعراق منطولي من معلم منا عمال معنى ولا بلا ما مع منه معروب مرد علما لعد العلي مرابع مع والرو معاد معاد معاد وسعلم و معر مراكرها كرباد والداد المرح وكر والم والرو والمعاد والروسل للمروا بعلى مسم مراكرها والمراج وكر والم والمع وحن والم مرابعا والمرابع العمادة المرابع مسم مراكرها والم والمراج وكر والم والمرو والمع وحن والم مرابعا والمرابع والروسل المروم والمحال

فراادله _ والحداله رد العالم ومطرا بدعام مدمج والد مع

لسمالد المحسب مراكر حسم وسالد الاست معدم الرحسم لهذه معالد مما ودخ علما مرت سمه وكان الود العرج الخلاصاس لهذه معالد مما ودخ علما مرت سمه وكان الوديد الحدل الاستولج مارس الكراليعماد ولتصار الدو ورم الغلل فالود الارسر السرال المنام الغلو الكراليعماد ولسعول وارال الوسوالما ولحم والما التحر والما المعالم المعالم المعاد وسعول وارال الوسوالما ولحم والما التحم والول الما المعالم

TOO	YBMF	OF	A	HOOW	TFIXH	IS	IOXWDEFBG
TOO	YBMF	ΟΚ	R	$\mathrm{H}\mathbf{O}\mathbf{O}\mathrm{W}$	T FQXH	QU	IOXWDEKBG
J 00	YBMF	OK	R	$\mathrm{H}\mathbf{O}\mathbf{O}\mathrm{W}$	JFQXH	QU	IOXWDEKBG
JNN	YBMF	NK	R	HNNW	JFQXH	QU	INXWDEKBG

The most common letters are E, T, A, O, I, N

Doubled letters: LL, EE, SS, OO

Digrams: letter pairs like QU that go together

Punctuation and spaces help a lot

دا معالده ما داليم وبصف والكلوم العنتي اعرة مرد الكال مريم مراسع له مر ما علم الد معاد سعد منه والع منطولي بنا معلم منا عواللم وسعد ولا بلا د ما معام الد معاد معاد والعراق منطولي من معلم منا عمال معنى ولا بلا ما مع منه معروب مرد علما لعد العلي مرابع مع والرو معاد معاد معاد وسعلم و معر مراكرها كرباد والداد المرح وكر والم والرو والمعاد والروسل للمروا بعلى مسم مراكرها والمراج وكر والم والمع وحن والم مرابعا والمرابع العمادة المرابع مسم مراكرها والم والمراج وكر والم والمرو والمع وحن والم مرابعا والمرابع والروسل المروم والمحال

فراادله _ والحداله رد العالم ومطرا بدعام مدمج والد مع

لسمالد المحسب مراكر حسم وسالد الاست معود ملي الدور واسترام المعرع للالعاس محد معالد مما ودخ علما مرت سمه وكان الودر الحدل الاستراح مارس التداريساء ولتصار الدو ورم النول فالوله الارسر السيال المنام المعول عناد الاسال لي المراجع المراذ ومعاليات خسر الموسود سايد المنام العول المامعاد وستول وارالوناو موهما: ولتر والما التقر واصل الما السيوالي

TOO	YBMH	OF	A	GOOD	THING	IS	IONDDEFBG
TOO	YBMF	OF	Α	$\mathrm{H}\mathbf{O}\mathbf{O}\mathrm{W}$	TFIXH	IS	IOXWDEFBG
TOO	YBMF	OK	R	$\mathrm{H}\mathbf{O}\mathbf{O}\mathrm{W}$	T FQXH	QU	IOXWDEKBG
J 00	YBMF	ΟΚ	R	$\mathrm{H}\mathbf{O}\mathbf{O}\mathrm{W}$	JFQXH	QU	IOXWDEKBG
JNN	YBMF	NK	R	HNNW	JFQXH	QU	INXWDEKBG

The most common letters are E, T, A, O, I, N

Doubled letters: LL, EE, SS, OO

Digrams: letter pairs like QU that go together

Punctuation and spaces help a lot

ذا سمالده ما داليم مصغه والكلوم العنتواحدة مره المالي مراجع ماليرلد مد ماغارات معارسه منعوا في منطقه محمد منا مواللم وسعد ولا بلا د مار مسلما واليلم ويلحونا والعليم الارضع فصطلما مسي وعلو به وسعله 3 مارح سير مراجعاً للم ويلحونا والعليم الارضع فصح السلد الميابعة والروسل المحرور المعلي مراجعاً المرداد و الداد المريخ دكن والد والرك ول حوالس الس الما العيادة الدام مد مراكحاً المرداد و الداد المريخ دكن والد والرك ول حوالي مراجعاً والرابعة مد مراكحاً المرداد والما والمريخ دكن والد والرك ول حوالي مراجعاً والروسل مد مراكحاً المرداد و الماد المريخ دكن والد والرك ول حوالي مراجعاً مراجعاً والروسية مد مراكحاً المرداد و الداد المريخ دكن والد والرك ول حوالي مراجعاً والمرابعة مد مراكحاً المرداد و المراجعة والمريخ وكن والد والمحمد والرك ول حوالي مراجعاً والمرابعة والمرابعة والمرابعة والم مد مراكماً المراد و المراجعة والمرجع والمحمد والمحمد مراكماً العيادة المرابعة و

فراادلد والحداله ردائعالم وطراب علم مدمجر والسدج

لسمايد المحسب مراكر حسم وسالد الاست يعور ملي والدور واستعرام المعرع لألانعاس محمد معاند مما ودفر علما مرت سمه وكان المودر الخدل الاستعرام مارس الكراليعساء ولتصاريل وور النول: فالموله الارسير السير المنام المعول عنها والا اسراد والمراك و ورم النول: فالموله الارسير اليون ورسير والمنام المعول المامعاد وستول واداد المنام ويواما: ولحم والمال العظم الما المستوالي

TOO	MUCH	OF	A	GOOD	THING	IS	WONDERFUL
TOO	YBMH	OF	A	GOOD	THING	IS	IONDDEFBG
тоо	YBMF	OF	A	$\mathrm{H}\mathbf{O}\mathbf{O}\mathrm{W}$	TFIXH	IS	IOXWDEFBG
TOO	YBMF	OK	R	$\mathrm{H}\mathbf{O}\mathbf{O}\mathrm{W}$	\mathbf{T} FQXH	QU	IOXWDEKBG
J 00	YBMF	OK	R	$\mathrm{H}\mathbf{O}\mathbf{O}\mathrm{W}$	JFQXH	QU	IOXWDEKBG
JNN	YBMF	NK	R	HNNW	JFQXH	QU	INXWDEKBG



Jefferson's cylinder

Each disk does a different scramble: the secret key is the order of the disks















Each letter changes the cipher, affecting the rest of the code, in a different way

Turing was a quite brilliant mathematician, most famous for his work on breaking the German Enigma codes. It is no exaggeration to say that, without his outstanding contribution, the history of the Second World War could have been very different.... The debt of gratitude he is owed makes it all the more horrifying, therefore, that he was treated so inhumanely. I am pleased to have the chance to say how deeply sorry I and we all are for what happened to him.



True security—but at a cost




One-time pad:



note: add mod 10 (no carries!)





One-time pad:



If the pad is truly random, the ciphertext is random too: No pattern that the codebreaker can discover

One-time pad:



If the pad is truly random, the ciphertext is random too: No pattern that the codebreaker can discover

But never use the same pad twice!

One-time pad:



note: add mod 10 (no carries!)

If the pad is truly random, the ciphertext is random too: No pattern that the codebreaker can discover

But never use the same pad twice!

Must share one digit of pad for every digit of message, and must do this in a physically secure way.



All of these methods encrypt one letter at a time

All of these methods encrypt one letter at a time

This lets us break them one letter at a time... like passwords in the movies

All of these methods encrypt one letter at a time

This lets us break them one letter at a time... like passwords in the movies

What we need is a method where every letter affects every other letter:

All of these methods encrypt one letter at a time

This lets us break them one letter at a time... like passwords in the movies

What we need is a method where every letter affects every other letter:



All of these methods encrypt one letter at a time

This lets us break them one letter at a time... like passwords in the movies

What we need is a method where every letter affects every other letter:



"*x* mod *N*" is the remainder when we divide *x* by *N*: for instance, *x* mod 10 is *x*'s 1s digit

"*x* mod *N*" is the remainder when we divide *x* by *N*: for instance, *x* mod 10 is *x*'s 1s digit

 $6+5 \mod 10 = 1$

"*x* mod *N*" is the remainder when we divide *x* by *N*: for instance, *x* mod 10 is *x*'s 1s digit

 $6+5 \mod 10 = 1$

 $11+3 \mod 12 = 2$



"*x* mod *N*" is the remainder when we divide *x* by *N*: for instance, *x* mod 10 is *x*'s 1s digit

 $6+5 \mod 10 = 1$

 $11+3 \mod 12 = 2$

24+3 mod 26 = 1: Y⇒B



" $x \mod N$ " is the remainder when we divide x by N: for instance, $x \mod 10$ is x's 1s digit

 $6+5 \mod 10 = 1$

 $11+3 \mod 12 = 2$

24+3 mod 26 = 1: Y⇒B

multiplication mod 5: $2 \times 3 = 1$

X	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

"*x* mod *N*" is the remainder when we divide *x* by *N*: for instance, *x* mod 10 is *x*'s 1s digit

 $6+5 \mod 10 = 1$

 $11+3 \mod 12 = 2$

24+3 mod 26 = 1: Y⇒B

multiplication mod 5: $2 \times 3 = 1$

 $75,764 \mod 1,000 = 764$







Anyone can send a message to Alice, but only she can decrypt it





Anyone can send a message to Alice, but only she can decrypt it

Alice publishes her public key: e, N





Anyone can send a message to Alice, but only she can decrypt it

Alice publishes her public key: e, N

To send Alice a message m, Bob encrypts it as $m^e \mod N$





Anyone can send a message to Alice, but only she can decrypt it

Alice publishes her public key: e, N

To send Alice a message m, Bob encrypts it as $m^e \mod N$

For example: *e*=3 and *N*=1,000





Anyone can send a message to Alice, but only she can decrypt it

Alice publishes her public key: e, N

To send Alice a message m, Bob encrypts it as $m^e \mod N$

For example: e=3 and N=1,000

To send Alice *m*=**413**, Bob encrypts it as











Alice's public key: e=3, N=1,000

To send Alice *m*=**413**, Bob encrypts it as

413³ = 413×413×413 = 70,444,**997**





Alice's public key: e=3, N=1,000

To send Alice *m*=**413**, Bob encrypts it as

413³ = 413×413×413 = 70,444,**997**

Only Alice knows that if we raise the encrypted message to the **67**th power, she gets the original message *m* back!





Alice's public key: e=3, N=1,000

To send Alice *m*=**413**, Bob encrypts it as

413³ = 413×413×413 = 70,444,**997**

Only Alice knows that if we raise the encrypted message to the **67**th power, she gets the original message *m* back!

997⁶⁷ =

817665373962643786759813699247646158630785787528904568618228 117721919932794531373761406228949504304716744619902823768572 754836451383036420378360358129864380547637845421151481946569 591385634343038032**413**





Alice's public key: e=3, N=1,000

To send Alice *m*=**413**, Bob encrypts it as

413³ = 413×413×413 = 70,444,**997**

Only Alice knows that if we raise the encrypted message to the **67**th power, she gets the original message *m* back!

caveat: *m* must be odd and not a multiple of 5

997⁶⁷ =

817665373962643786759813699247646158630785787528904568618228 117721919932794531373761406228949504304716744619902823768572 754836451383036420378360358129864380547637845421151481946569 591385634343038032**413**








Alice's public key: *e*=3, *N*=1000





Alice's public key: *e*=3, *N*=1000

Her private key: *d*=67





Alice's public key: *e*=3, *N*=1000

Her private key: *d*=67

Can we crack her code?





Alice's public key: *e*=3, *N*=1000

Her private key: *d*=67

Can we crack her code?

Can we get *d* from *e* and *N*?





Alice's public key: *e*=3, *N*=1000

Her private key: *d*=67

Can we crack her code?

Can we get *d* from *e* and *N*?

We can do this if we can factor *N*, break it down into a product of prime numbers: 2, 3, 5, 7, 11, 13, 17, 19...





Alice's public key: e=3, N=1000

Her private key: *d*=67

Can we crack her code?

Can we get *d* from *e* and *N*?

We can do this if we can factor *N*, break it down into a product of prime numbers: 2, 3, 5, 7, 11, 13, 17, 19...

For instance, $1000 = 2 \times 2 \times 5 \times 5 \times 5$





Multiplying is easy

Multiplying is easy

We have an *algorithm* that multiplies *n*-digit numbers in about $n \times n = n^2$ time

Multiplying is easy

We have an *algorithm* that multiplies *n*-digit numbers in about $n \times n = n^2$ time



Multiplying is easy

We have an *algorithm* that multiplies *n*-digit numbers in about $n \times n = n^2$ time



Multiplication is in the class P of problems that can be solved in *polynomial time*



Is $2^{67}-1 = 147,573,952,588,676,412,927$ a prime?



Is $2^{67}-1 = 147,573,952,588,676,412,927$ a prime?

No, because it's 193707721×761838257287



Is $2^{67}-1 = 147,573,952,588,676,412,927$ a prime?

No, because it's 193707721×761838257287

Factoring is in the class NP of problems where we can *check* a solution in polynomial time...



Is $2^{67}-1 = 147,573,952,588,676,412,927$ a prime?

No, because it's 193707721×761838257287

Factoring is in the class NP of problems where we can *check* a solution in polynomial time...

...but that doesn't mean we can find one!





Is $2^{67}-1 = 147,573,952,588,676,412,927$ a prime?

No, because it's 193707721×761838257287

Factoring is in the class NP of problems where we can *check* a solution in polynomial time...

...but that doesn't mean we can find one!

We believe (but don't know) that factoring *n*-digit numbers takes *exponential* time













Until the end of the world



The usual kind of computation looks like this:



The usual kind of computation looks like this:

A randomized computation looks like this:



The usual kind of computation looks like this:

A randomized computation looks like this:

Each path has a probability



The usual kind of computation looks like this:

A randomized computation looks like this:

Each path has a probability



The usual kind of computation looks like this:

A randomized computation looks like this:

Each path has a probability

The total probability of getting the right answer is the sum of the probabilities of the paths that lead there



The usual kind of computation looks like this:

A randomized computation looks like this:

Each path has a probability

The total probability of getting the right answer is the sum of the probabilities of the paths that lead there

Some of our best algorithms work this way! (Like telling whether or not a number is prime)



Enter the quantum

Probability is a number between 0 and 1; different possibilities add up

But waves have both *amplitude* and *phase*: they can add or cancel









The two-slit experiment

The two-slit experiment

Thomas Young, 1801: "light is possessed of opposite qualities, capable of neutralising or destroying each other."



The two-slit experiment

Thomas Young, 1801: "light is possessed of opposite qualities, capable of neutralising or destroying each other."



We see this even with one electron at a time! Even one particle is like a wave

In two places at once



In two places at once

There are two paths the electron can take to each location


There are two paths the electron can take to each location

If these paths have the same "phase", the paths add, and the probability is high



There are two paths the electron can take to each location

If these paths have the same "phase", the paths add, and the probability is high

If they have opposite phase, they cancel



There are two paths the electron can take to each location

If these paths have the same "phase", the paths add, and the probability is high

If they have opposite phase, they cancel

You can get to x' from A or B—and you never show up there at all!



There are two paths the electron can take to each location

If these paths have the same "phase", the paths add, and the probability is high

If they have opposite phase, they cancel

You can get to x' from A or B—and you never show up there at all!

Idea of quantum computation: probability adds up at the right answer, cancels out at the wrong ones





Take the powers of some number x mod N, and see when this sequence repeats: 1, x, x^2 , x^3 ...



Take the powers of some number x mod N, and see when this sequence repeats: 1, x, x^2 , x^3 ...



Take the powers of some number x mod N, and see when this sequence repeats: 1, x, x^2 , x^3 ...

$$t: 0 1 2 3 4 5 6 7 8$$
$$2^{t}: 1 2 4 8 1 2 4 8 1$$
$$2^{4} = 15 + 1$$



Take the powers of some number x mod N, and see when this sequence repeats: 1, x, x^2 , x^3 ...



Take the powers of some number x mod N, and see when this sequence repeats: 1, x, x^2 , x^3 ...

$$t: 0 1 2 3 4 5 6 7 8$$

$$2^{t}: 1 2 4 8 1 2 4 8 1$$

$$16 - 1 = 15$$

$$4^{2} - 1^{2} = 15$$



Take the powers of some number x mod N, and see when this sequence repeats: 1, x, x^2 , x^3 ...



$$t: 0 1 2 3 4 5 6 7 8$$

$$2^{t}: 1 2 4 8 1 2 4 8 1$$

$$16-1=15$$

$$4^{2}-1^{2}=15$$

$$x^{2}-y^{2}=(x-y)(x+y)$$

Take the powers of some number x mod N, and see when this sequence repeats: 1, x, x^2 , x^3 ...



$$t: 0 1 2 3 4 5 6 7 8$$

$$2^{t}: 1 2 4 8 1 2 4 8 1$$

$$16-1=15$$

$$4^{2}-1^{2}=15$$

$$x^{2}-y^{2}=(x-y)(x+y)$$

$$(4-1)\times(4+1)=15$$

Take the powers of some number x mod N, and see when this sequence repeats: 1, x, x^2 , x^3 ...



$$t: 0 1 2 3 4 5 6 7 8$$

$$2^{t}: 1 2 4 8 1 2 4 8 1$$

$$16-1=15$$

$$4^{2}-1^{2}=15$$

$$x^{2}-y^{2}=(x-y)(x+y)$$

$$(4-1)\times(4+1)=15$$

$$3\times5=15$$



Take the powers of some number x mod N, and see when this sequence repeats: 1, x, x^2 , x^3 ...

nis

For instance, to factor N = 15, look at the powers of 2:

$$t: 0 1 2 3 4 5 6 7 8$$

$$2^{t}: 1 2 4 8 1 2 4 8 1$$

$$16-1=15$$

$$4^{2}-1^{2}=15$$

$$x^{2}-y^{2}=(x-y)(x+y)$$

$$(4-1)\times(4+1)=15$$

$$3\times5=15$$

But if the list of powers is very long, how can we tell when it repeats?



















Fourier analysis breaks a signal down into a sum of frequencies





A quantum algorithm can pick out the frequencies in a sequence of numbers, even if it's exponentially long!



Fourier analysis breaks a signal down into a sum of frequencies





A quantum algorithm can pick out the frequencies in a sequence of numbers, even if it's exponentially long!

This means they can factor large numbers...



Fourier analysis breaks a signal down into a sum of frequencies





A quantum algorithm can pick out the frequencies in a sequence of numbers, even if it's exponentially long!

This means they can factor large numbers...

and break RSA cryptography



What next?

What next?

Are there cryptosystems that even quantum computers can't break?

What next?

Are there cryptosystems that even quantum computers can't break?

Are there problems that even quantum computers can't solve?

0	0	0	1	1	1	1
0	1	1	0	0	1	1
1	0	1	0	1	0	1

$$\begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$
$$\begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 0 \end{bmatrix}$$

A set of possible messages, with large differences between every pair of possibilities

$$\begin{bmatrix} 0\\1\\1\\1 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1\\ 0 & 1 & 1 & 0 & 0 & 1 & 1\\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$
$$\begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 0 \end{bmatrix}$$

Every combination is at least 4 bits different from every other one: if any one bit gets flipped, we can fix it



A set of possible messages, with large differences between every pair of possibilities

$$\begin{bmatrix} 0\\1\\1\\1 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1\\ 0 & 1 & 1 & 0 & 0 & 1 & 1\\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$
$$\begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 0 \end{bmatrix}$$

Every combination is at least 4 bits different from every other one: if any one bit gets flipped, we can fix it

A crystal of codewords: in high dimensions, finding the closest one is NP-hard—a needle in a haystack





A set of possible messages, with large differences between every pair of possibilities

$$\begin{bmatrix} 0\\1\\1\\1 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1\\ 0 & 1 & 1 & 0 & 0 & 1 & 1\\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$
$$\begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 0 \end{bmatrix}$$

Every combination is at least 4 bits different from every other one: if any one bit gets flipped, we can fix it

A crystal of codewords: in high dimensions, finding the closest one is NP-hard—a needle in a haystack

But for some special codes, we can do this quickly







The McEliece cryptosystem





The McEliece cryptosystem

Alice has an error-correcting code in which she can correct errors easily





The McEliece cryptosystem

Alice has an error-correcting code in which she can correct errors easily

She publishes a scrambled version of it, twisting and turning the crystal in order to make it look unfamiliar




The McEliece cryptosystem

Alice has an error-correcting code in which she can correct errors easily

She publishes a scrambled version of it, twisting and turning the crystal in order to make it look unfamiliar

Bob composes his message in the scrambled code, adds some noise, and sends it





The McEliece cryptosystem

Alice has an error-correcting code in which she can correct errors easily

She publishes a scrambled version of it, twisting and turning the crystal in order to make it look unfamiliar

Bob composes his message in the scrambled code, adds some noise, and sends it

Removing Bob's noise is hard for an eavesdropper (we hope), but easy for Alice





Even if we know Alice's internal code, how can we tell how she scrambled it?

Even if we know Alice's internal code, how can we tell how she scrambled it?

Similar: can I rearrange these nodes to turn one network into the other?



Even if we know Alice's internal code, how can we tell how she scrambled it?

Similar: can I rearrange these nodes to turn one network into the other?



We don't know how to solve this problem on classical computers... What about quantum ones?

Emmy Noether: physics is about symmetry



Emmy Noether: physics is about symmetry

Einstein: symmetries of space-time are not what Galileo thought they were



Emmy Noether: physics is about symmetry

Einstein: symmetries of space-time are not what Galileo thought they were

Periodicity is symmetry: shift and it stays the same



Emmy Noether: physics is about symmetry

Einstein: symmetries of space-time are not what Galileo thought they were

Periodicity is symmetry: shift and it stays the same



Emmy Noether: physics is about symmetry

Einstein: symmetries of space-time are not what Galileo thought they were

Periodicity is symmetry: shift and it stays the same

Higher-dimensional symmetries:



Emmy Noether: physics is about symmetry

Einstein: symmetries of space-time are not what Galileo thought they were

Periodicity is symmetry: shift and it stays the same

Higher-dimensional symmetries:





Emmy Noether: physics is about symmetry

Einstein: symmetries of space-time are not what Galileo thought they were

Periodicity is symmetry: shift and it stays the same

Higher-dimensional symmetries:





Can quantum computers detect the symmetries of these graphs — the rearrangements that turn them into each other?



Can quantum computers detect the symmetries of these graphs — the rearrangements that turn them into each other?









Scramblings of codes or networks are *permutations*



Scramblings of codes or networks are *permutations*

We can "multiply" them, but $xy \neq yx$





Scramblings of codes or networks are *permutations*

We can "multiply" them, but $xy \neq yx$



Like a Rubik's cube: order of rotations matters



From permutations to rotations

From permutations to rotations

Every group of permutations can be represented by rotations and reflections in a high-dimensional space

From permutations to rotations

Every group of permutations can be represented by rotations and reflections in a high-dimensional space

Permute the five colors:



The ways Alice can scramble her code correspond to rotations and reflections in a very (exponentially!) high-dimensional space

The ways Alice can scramble her code correspond to rotations and reflections in a very (exponentially!) high-dimensional space

If we try to use a method like Shor's, the algorithm "gets lost" in these spaces

The ways Alice can scramble her code correspond to rotations and reflections in a very (exponentially!) high-dimensional space

If we try to use a method like Shor's, the algorithm "gets lost" in these spaces

Any quantum measurement we try to do gives nearly the same result no matter what scrambling Alice used...

The ways Alice can scramble her code correspond to rotations and reflections in a very (exponentially!) high-dimensional space

If we try to use a method like Shor's, the algorithm "gets lost" in these spaces

Any quantum measurement we try to do gives nearly the same result no matter what scrambling Alice used...

...so we learn next to nothing about how to crack her code

To show that we can crack a code, one algorithm is enough

To show that we can crack a code, one algorithm is enough

But to prove that we can't, we have to reason about all possible algorithms

To show that we can crack a code, one algorithm is enough

But to prove that we can't, we have to reason about all possible algorithms

Factoring, and breaking RSA, might be easy for classical computers: maybe we just haven't been clever enough to think of an algorithm! (We've been surprised before.)

To show that we can crack a code, one algorithm is enough

But to prove that we can't, we have to reason about all possible algorithms

Factoring, and breaking RSA, might be easy for classical computers: maybe we just haven't been clever enough to think of an algorithm! (We've been surprised before.)

But any quantum algorithm that breaks the McEliece cryptosystem would have to use completely new ideas...

Alice, Bob, and Eve





Alice, Bob, and Eve







Alice, Bob, and Eve



If Eve measures Alice's message, this disturbs it in a way that Alice and Bob can detect
Alice, Bob, and Eve



If Eve measures Alice's message, this disturbs it in a way that Alice and Bob can detect

If their message got through without being intercepted, they can use it as a secret key [Bennett and Brassard, 1984]



Alice, Bob, and Eve



If Eve measures Alice's message, this disturbs it in a way that Alice and Bob can detect

If their message got through without being intercepted, they can use it as a secret key [Bennett and Brassard, 1984]

144 km between the Canary Islands, and over 300 km of optical fiber: bank transfers and election results in Geneva



The first transistor looked like this:



The first transistor looked like this:

Now they look like this:





The first transistor looked like this:

Now they look like this:



100 nm



The first integrated circuit looked like this:



The first integrated circuit looked like this:

Now they look like this:





We are rapidly gaining an ability to manipulate single atoms

We are rapidly gaining an ability to manipulate single atoms





We are rapidly gaining an ability to manipulate single atoms





We are rapidly gaining an ability to manipulate single atoms

Quantum computation is delicate: we need strong interactions in order to compute, but we have to avoid stray interactions that "measure" and destroy the quantum state





We are rapidly gaining an ability to manipulate single atoms

Quantum computation is delicate: we need strong interactions in order to compute, but we have to avoid stray interactions that "measure" and destroy the quantum state





We are rapidly gaining an ability to manipulate single atoms

Quantum computation is delicate: we need strong interactions in order to compute, but we have to avoid stray interactions that "measure" and destroy the quantum state



We are rapidly gaining an ability to manipulate single atoms

Quantum computation is delicate: we need strong interactions in order to compute, but we have to avoid stray interactions that "measure" and destroy the quantum state



We are rapidly gaining an ability to manipulate single atoms

Quantum computation is delicate: we need strong interactions in order to compute, but we have to avoid stray interactions that "measure" and destroy the quantum state



We are rapidly gaining an ability to manipulate single atoms

Quantum computation is delicate: we need strong interactions in order to compute, but we have to avoid stray interactions that "measure" and destroy the quantum state

This is challenging, but not impossible: simple quantum devices are now being built

It will take a while for this...



We are rapidly gaining an ability to manipulate single atoms

Quantum computation is delicate: we need strong interactions in order to compute, but we have to avoid stray interactions that "measure" and destroy the quantum state

This is challenging, but not impossible: simple quantum devices are now being built

It will take a while for this...

To turn into this





Shameless Plug



www.nature-of-computation.org

To put it bluntly: this book rocks! It somehow manages to combine the fun of a popular book with the intellectual heft of a textbook. Scott Aaronson, MIT

This is, simply put, the best-written book on the theory of computation I have ever read; one of the best-written mathematical books I have ever read, period.

Cosma Shalizi, Carnegie Mellon