




























<p>100% talks, 0% human interaction.</p> 	<p>16-bit AES.</p> 	<p>17 slides for a 3-minute rump session talk.</p> 
<p>2 to 4 kilograms of top quality amphetamines.</p> 	<p>2-sentence Eurocrypt reviews.</p> 	<p>387 contact tracing papers submitted to Eurocrypt 2021.</p> 
<p>4mm reasonable margins.</p> 	<p>A 25-year old policy on sexual harassment.</p> 	<p>A Facebook friend request from a cryptographer I actually despise.</p> 










Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography

<p>A career-limiting card game.</p> 	<p>A dancing cryptographer.</p> 	<p>A genuine attempt to configure IPsec.</p> 
<p>A hand wavy argument.</p> 	<p>A long-term nonce.</p> 	<p>A non-fabricated use of pairings.</p> 
<p>A painfully slow Tor masturbation session.</p> 	<p>A popup Skype notification from “lovemachine69” during my keynote talk.</p> 	<p>A proof that appears in the “full version”.</p> 










Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography

<p>A shepherd that won't budge.</p> 	<p>A tight security reduction to the problem of fending off a sexually voracious goat.</p> 	<p>A violent and bloody PhD defence.</p> 
<p>Aaron Aaronson's insistence on alphabetical author ordering.</p> 	<p>Academic integrity.</p> 	<p>Accidentally sexting my co-supervisor.</p> 
<p>Actually being "sorry for the late reply".</p> 	<p>Actually efficient indistinguishability obfuscation.</p> 	<p>Adleman-Rivest-Shamir encryption (the ARSE algorithm).</p> 










Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography

<p>An IACR board meeting.</p> 	<p>An SSL vulnerability with a silly name.</p> 	<p>An “anonymous” reviewer insisting I cite 6 papers by the same author.</p> 
<p>An inappropriate workplace romance.</p> 	<p>An insecure VPN straight to the Kremlin.</p> 	<p>An overfull hbox.</p> 
<p>An overlooked patent.</p> 	<p>Arguing savagely against contact tracing so no one finds out that I don’t get invited to parties.</p> 	<p>Arriving 13 minutes late to a 15 minute talk and having the gall to ask a question.</p> 










Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography

<p>Asking for 2 room keys during check-in, knowing full well I'm not getting laid.</p> 	<p>Bart Preneel's private key.</p> 	<p>Beefing up my Proposition to a Theorem because I'm that awesome.</p> 
<p>Being forced to attend social events because I'm the visitor's official host.</p> 	<p>Being the only smartly dressed person in the room.</p> 	<p>Best rejected paper award.</p> 
<p>Bragging about getting held up at Border Control for saying I'm a cryptographer.</p> 	<p>Brexit.</p> 	<p>Checking my Google Scholar profile daily.</p> 










Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography

<p>Chocolate-covered shrimp.</p> 	<p>Citing personal communication.</p> 	<p>Conferences with 5 submissions at 11:59pm.</p> 
<p>Crippling student debt.</p> 	<p>Crypto wars.</p> 	<p>Day drinking.</p> 
<p>Deadline day flatulence.</p> 	<p>Deliberately hiding inefficiencies inside the big O.</p> 	<p>Deliberately not referencing a superior paper.</p> 










Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography

<p>Desperately trying to plug my crypto research into a grant application on pandemic prevention.</p> 	<p>Diffie but definitely not Hellman.</p> 	<p>Doing Facebook maths puzzles to show I am better than those idiot 97%.</p> 
<p>Double ROT-13.</p> 	<p>Drinking alone.</p> 	<p>Dropping the word Blockchain into my research proposal as many times as possible.</p> 
<p>Dual_EC_DRBG.</p> 	<p>Encrypted database security definitions.</p> 	<p>Explaining what my job is at a family reunion.</p> 










Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography

<p>Falling asleep in a 5-person meeting.</p> 	<p>Feeling flattered because a conference spam email addressed me as Professor.</p> 	<p>Fighting over LaTeX syntax.</p> 
<p>Filing a patent application for modular multiplication... in 2017.</p> 	<p>Flirting with people at the conference registration desk.</p> 	<p>Forgetting my VGA adapter.</p> 
<p>Frantically taking notes during every talk.</p> 	<p>GDPR requirements.</p> 	<p>Getting a fourth cookie during a coffee break because I have no one to talk to.</p> 










Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography

<p>Getting rejected, but then taking immediate solace in the fact that the selection of papers was a difficult and challenging task.</p> 	<p>Getting stuck at the French-speaking banquet table.</p> 	<p>Getting tenure, then chilling the f— right out!</p> 
<p>Getting turned on by a proof.</p> 	<p>Going straight to journal.</p> 	<p>Government-mandated backdoors.</p> 
<p>HTTPS everywhere!</p> 	<p>Hands-on supervision.</p> 	<p>Having time to catch up on my reading, then not doing it.</p> 










Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography

<p>Having to wear pants.</p> 	<p>Having to write a polite rebuttal to the reviewer who clearly didn't read past page 2.</p> 	<p>Hiding my conflict of interest.</p> 
<p>Hillary Clinton's BlackBerry.</p> 	<p>Home-baked, snake oil crypto.</p> 	<p>Ignoring reviewer comments and resubmitting immediately.</p> 
<p>Ignoring the session chair flashing 5 minutes left because I've got 23 slides to go.</p> 	<p>Including an XKCD comic in my slides because I'm so original.</p> 	<p>Knapsack cryptosystems, revisited.</p> 










Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography

<p>LNCS' 25-foot margins.</p> 	<p>Making claims in the submission that you hope you can achieve before the rebuttal.</p> 	<p>Maths-terbation.</p> 
<p>My Silk Road purchase history.</p> 	<p>My h-index.</p> 	<p>My automated reply saying “email responses will be delayed”, when I know damn well I’ll be online with high-speed internet access 24/7.</p> 
<p>My butt.</p> 	<p>My crypto blog views getting into the double digits.</p> 	<p>My dear friend the Program Chair overruling 3 borderline rejects on my paper.</p> 

Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography

<p>My genitals.</p> 	<p>My inappropriate supervisor.</p> 	<p>My inflated sense of self-importance that warrants my PGP key.</p> 
<p>My much more successful career as a singer after rocking the Crypto rump session.</p> 	<p>My relationship status.</p> 	<p>My second divorce.</p> 
<p>My sex life.</p> 	<p>My side job as an incompetent security consultant.</p> 	<p>My successful career at a patent troll company.</p> 

Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography

<p>My supervisor's morning breath.</p> 	<p>Nigel Smart's new Hawaiian shirt.</p> 	<p>Not being important enough to be asked to sign the public statement on contact tracing.</p> 
<p>Not feeling guilty about falling asleep during the keynote.</p> 	<p>Not having to wear pants.</p> 	<p>Not needing to pretend to listen to the other speakers in my session.</p> 
<p>Overselling it hard in the introduction.</p> 	<p>Password1.</p> 	<p>Picturing the FSE audience naked.</p> 

**Cards
Against
Cryptography**

**Cards
Against
Cryptography**

**Cards
Against
Cryptography**

**Cards
Against
Cryptography**










**Cards
Against
Cryptography**

**Cards
Against
Cryptography**



**Cards
Against
Cryptography**

**Cards
Against
Cryptography**










**Cards
Against
Cryptography**

<p>Politely starting an answer with “That’s a good question...”, when the question is actually idiotic.</p> 	<p>Post-quantum RSA.</p> 	<p>Preparing for two weeks to give a 15-minute presentation to a room of 7 people all on their laptops.</p> 
<p>Pretending to care when my vegetarian coauthor complains about the lack of banquet options.</p> 	<p>Pretending to understand.</p> 	<p>Pubic key cryptography.</p> 
<p>Publishing anyway.</p> 	<p>Purchasing the Springer hardcopies I publish in because my mom is collecting them.</p> 	<p>Putting an outdoors-y photo on my academic webpage to look well-rounded.</p> 










Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography

<p>Quadruple XOR.</p> 	<p>Quantum key distribution.</p> 	<p>Quickly trying to peek at someone's badge as I shake their hand, but it's flipped backwards.</p> 
<p>Reading the person in front's emails.</p> 	<p>Relatives who ask me to help them install their printer on Windows.</p> 	<p>Remembering when 'working from home' meant a day off.</p> 
<p>Rogaway's loose morals.</p> 	<p>Satoshi Nakamoto.</p> 	<p>Security through obscurity.</p> 










Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography

<p>Sending an email at 11pm so people think I work hard.</p> 	<p>Serious rump session speakers.</p> 	<p>Sexual tension.</p> 
<p>Skype dropping out every 10 to 15 seconds.</p> 	<p>Social sciences.</p> 	<p>Someone less senior than me signing off with “Thanks in advance”.</p> 
<p>Spending 3 Bitcoin on pizza in 2012.</p> 	<p>Spending all of my Levchin prize money on cocaine.</p> 	<p>Springer’s editorial team.</p> 










Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography

<p>Starting a conversation with “When did you fly in?”, because I have nothing interesting to say.</p> 	<p>Taking a group shower with my recent co-authors.</p> 	<p>Telling anyone who’ll listen quite how busy I am.</p> 
<p>Thanking the anonymous reviewers for their “useful” comments.</p> 	<p>That feeling when my article is sitting pretty at the top of the ePrint archive.</p> 	<p>That one asshole who’s always sleeping during my Eurocrypt talks.</p> 
<p>The MIT Mafia.</p> 	<p>The NSA’s massive stack of amateur porn.</p> 	<p>The North Korean Cryptographic Standard.</p> 










Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography

<p>The awkward question the chair asks when nobody understood the talk.</p> 	<p>The awkward silence of 8 people standing in a circle during the afternoon coffee break.</p> 	<p>The great firewall of China.</p> 
<p>The great paywall of IEEE.</p> 	<p>The intoxicating aroma of 12 PhD students in one office.</p> 	<p>The latest dance mix album by DJ Bernstein.</p> 
<p>The one person I don't want to get stuck next to on the conference excursion bus.</p> 	<p>The one really hot person at CHES registration drinks.</p> 	<p>The one suit I own for meetings with industry.</p> 










Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography

<p>The person in the front row taking photos of every slide.</p> 	<p>The secret flash drive hidden in my underwear.</p> 	<p>The sound of 50 people on a Zoom call all trying to speak at once.</p> 
<p>The student body.</p> 	<p>The walking zombie corpse of Claude Shannon.</p> 	<p>Thinking I'm so clever for using pictures of Alice (Cooper) and Bob (Marley).</p> 
<p>Throwing a party for my next citation milestone.</p> 	<p>Trying to make TCC friends at the bar in order to get the IACR 7-conference grand slam.</p> 	<p>Turbulent bowel movements in the middle of my Asiacrypt presentation.</p> 

Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography

<p>Turning up to one meeting and claiming co-authorship.</p> 	<p>Tweeting about my paper acceptance.</p> 	<p>Unbreakable military-grade encryption.</p> 
<p>Undergrads.</p> 	<p>Using Beamer because it's social suicide to use PowerPoint.</p> 	<p>Using “it clearly follows” when the implied following is anything but clear.</p> 
<p>Using “we should talk about this offline” because the question exposes holes in my paper.</p> 	<p>Using indecipherable, non-standard notation to hide a dodgy proof.</p> 	<p>Vital sugar beet auctions.</p> 

Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography

<p>WalnutDSA.</p> 	<p>Wearing a T-shirt with a Linux joke.</p> 	<p>Wearing a conference t-shirt... in public.</p> 
<p>When you realize that quantum computers have been 10 years away for 3 decades.</p> 	<p>Wistfully looking out of the window of my overly-cramped PhD office.</p> 	<p>Writing a reference for someone I can't remember meeting.</p> 
<p>Yet another cryptographer falling into the blockchain startup abyss.</p> 	<p>Ctrl+F'ing to see how many times I'm cited and finding "0 results".</p> 	<p>"Working" remotely.</p> 

Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography

**A slide deck entirely in
Comic Sans.**



Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography