










<p><b>16-bit AES.</b></p> 	<p><b>17 slides for a 3-minute rump session talk.</b></p> 	<p><b>2 to 4 kilograms of top quality amphetamines.</b></p> 
<p><b>2-sentence Eurocrypt reviews.</b></p> 	<p><b>4mm reasonable margins.</b></p> 	<p><b>A 25-year old policy on sexual harassment.</b></p> 
<p><b>A Facebook friend request from a cryptographer I actually despise.</b></p> 	<p><b>A career-limiting card game.</b></p> 	<p><b>A dancing cryptographer.</b></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><b>A genuine attempt to configure IPsec.</b></p> 	<p><b>A hand wavy argument.</b></p> 	<p><b>A long-term nonce.</b></p> 
<p><b>A non-fabricated use of pairings.</b></p> 	<p><b>A painfully slow Tor masturbation session.</b></p> 	<p><b>A popup Skype notification from “lovemachine69” during my keynote talk.</b></p> 
<p><b>A proof that appears in the “full version”.</b></p> 	<p><b>A shepherd that won’t budge.</b></p> 	<p><b>A tight security reduction to the problem of fending off a sexually voracious goat.</b></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><b>A violent and bloody PhD defence.</b></p> 	<p><b>Aaron Aaronson's insistence on alphabetical author ordering.</b></p> 	<p><b>Academic integrity.</b></p> 
<p><b>Accidentally sexting my co-supervisor.</b></p> 	<p><b>Actually being "sorry for the late reply".</b></p> 	<p><b>Actually efficient indistinguishability obfuscation.</b></p> 
<p><b>Adleman-Rivest-Shamir encryption (the ARSE algorithm).</b></p> 	<p><b>An IACR board meeting.</b></p> 	<p><b>An SSL vulnerability with a silly name.</b></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><b>An “anonymous” reviewer insisting I cite 6 papers by the same author.</b></p> 	<p><b>An inappropriate workplace romance.</b></p> 	<p><b>An insecure VPN straight to the Kremlin.</b></p> 
<p><b>An overfull hbox.</b></p> 	<p><b>An overlooked patent.</b></p> 	<p><b>Arriving 13 minutes late to a 15 minute talk and having the gall to ask a question.</b></p> 
<p><b>Asking for 2 room keys during check-in, knowing full well I’m not getting laid.</b></p> 	<p><b>Bart Preneel’s private key.</b></p> 	<p><b>Beefing up my Proposition to a Theorem because I’m that awesome.</b></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><b>Being forced to attend social events because I'm the visitor's official host.</b></p> 	<p><b>Being the only smartly dressed person in the room.</b></p> 	<p><b>Best rejected paper award.</b></p> 
<p><b>Bragging about getting held up at Border Control for saying I'm a cryptographer.</b></p> 	<p><b>Brexit.</b></p> 	<p><b>Checking my Google Scholar profile daily.</b></p> 
<p><b>Chocolate-covered shrimp.</b></p> 	<p><b>Citing personal communication.</b></p> 	<p><b>Conferences with 5 submissions at 11:59pm.</b></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><b>Crippling student debt.</b></p> 	<p><b>Crypto wars.</b></p> 	<p><b>Deadline day flatulence.</b></p> 
<p><b>Deliberately hiding inefficiencies inside the big O.</b></p> 	<p><b>Deliberately not referencing a superior paper.</b></p> 	<p><b>Diffie but definitely not Hellman.</b></p> 
<p><b>Doing Facebook maths puzzles to show I am better than those idiot 97%.</b></p> 	<p><b>Double ROT-13.</b></p> 	<p><b>Drinking alone.</b></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><b>Dropping the word Blockchain into my research proposal as many times as possible.</b></p> 	<p><b>Dual_EC_DRBG.</b></p> 	<p><b>Encrypted database security definitions.</b></p> 
<p><b>Explaining what my job is at a family reunion.</b></p> 	<p><b>Falling asleep in a 5-person meeting.</b></p> 	<p><b>Feeling flattered because a conference spam email addressed me as Professor.</b></p> 
<p><b>Fighting over LaTeX syntax.</b></p> 	<p><b>Filing a patent application for modular multiplication... in 2017.</b></p> 	<p><b>Flirting with people at the conference registration desk.</b></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><b>Forgetting my VGA adapter.</b></p> 	<p><b>Frantically taking notes during every talk.</b></p> 	<p><b>GDPR requirements.</b></p> 
<p><b>Getting a fourth cookie during a coffee break because I have no one to talk to.</b></p> 	<p><b>Getting rejected, but then taking immediate solace in the fact that the selection of papers was a difficult and challenging task.</b></p> 	<p><b>Getting stuck at the French-speaking banquet table.</b></p> 
<p><b>Getting tenure, then chilling the f— right out!</b></p> 	<p><b>Getting turned on by a proof.</b></p> 	<p><b>Going straight to journal.</b></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><b>Government-mandated backdoors.</b></p> 	<p><b>HTTPS everywhere!</b></p> 	<p><b>Hands-on supervision.</b></p> 
<p><b>Having to write a polite rebuttal to the reviewer who clearly didn't read past page 2.</b></p> 	<p><b>Hiding my conflict of interest.</b></p> 	<p><b>Hillary Clinton's BlackBerry.</b></p> 
<p><b>Home-baked, snake oil crypto.</b></p> 	<p><b>Ignoring reviewer comments and resubmitting immediately.</b></p> 	<p><b>Ignoring the session chair flashing 5 minutes left because I've got 23 slides to go.</b></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><b>Including an XKCD comic in my slides because I'm so original.</b></p> 	<p><b>Knapsack cryptosystems, revisited.</b></p> 	<p><b>LNCS' 25-foot margins.</b></p> 
<p><b>Making claims in the submission that you hope you can achieve before the rebuttal.</b></p> 	<p><b>Maths-terbation.</b></p> 	<p><b>My Silk Road purchase history.</b></p> 
<p><b>My <i>h</i>-index.</b></p> 	<p><b>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.</b></p> 	<p><b>My butt.</b></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><b>My crypto blog views getting into the double digits.</b></p> 	<p><b>My dear friend the Program Chair overruling 3 borderline rejects on my paper.</b></p> 	<p><b>My genitals.</b></p> 
<p><b>My inappropriate supervisor.</b></p> 	<p><b>My inflated sense of self-importance that warrants my PGP key.</b></p> 	<p><b>My much more successful career as a singer after rocking the Crypto rump session.</b></p> 
<p><b>My relationship status.</b></p> 	<p><b>My second divorce.</b></p> 	<p><b>My sex life.</b></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><b>My side job as an incompetent security consultant.</b></p> 	<p><b>My successful career at a patent troll company.</b></p> 	<p><b>My supervisor's morning breath.</b></p> 
<p><b>Nigel Smart's new Hawaiian shirt.</b></p> 	<p><b>Overselling it hard in the introduction.</b></p> 	<p><b>Password1.</b></p> 
<p><b>Picturing the FSE audience naked.</b></p> 	<p><b>Politely starting an answer with "That's a good question...", when the question is actually idiotic.</b></p> 	<p><b>Post-quantum RSA.</b></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><b>Preparing for two weeks to give a 15-minute presentation to a room of 7 people all on their laptops.</b></p> 	<p><b>Pretending to care when my vegetarian coauthor complains about the lack of banquet options.</b></p> 	<p><b>Pretending to understand.</b></p> 
<p><b>Pubic key cryptography.</b></p> 	<p><b>Publishing anyway.</b></p> 	<p><b>Purchasing the Springer hardcopies I publish in because my mom is collecting them.</b></p> 
<p><b>Putting an outdoors-y photo on my academic webpage to look well-rounded.</b></p> 	<p><b>Quadruple XOR.</b></p> 	<p><b>Quantum key distribution.</b></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><b>Quickly trying to peek at someone's badge as I shake their hand, but it's flipped backwards.</b></p> 	<p><b>Reading the person in front's emails.</b></p> 	<p><b>Relatives who ask me to help them install their printer on Windows.</b></p> 
<p><b>Rogaway's loose morals.</b></p> 	<p><b>Satoshi Nakamoto.</b></p> 	<p><b>Security through obscurity.</b></p> 
<p><b>Sending an email at 11pm so people think I work hard.</b></p> 	<p><b>Serious rump session speakers.</b></p> 	<p><b>Sexual tension.</b></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**

**Skype dropping  
out every 10 to 15  
seconds.**



**Social sciences.**



**Someone less senior  
than me signing  
off with “Thanks in  
advance”.**



**Spending 3 Bitcoin on  
pizza in 2012.**



**Spending all of my  
Levchin prize money  
on cocaine.**



**Springer’s editorial  
team.**



**Starting a  
conversation with  
“When did you fly  
in?”, because I have  
nothing interesting to  
say.**



**Taking a group shower  
with my recent co-  
authors.**



**Telling anyone who’ll  
listen quite how busy  
I am.**



**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**

**Thanking the anonymous reviewers for their “useful” comments.**



**That feeling when my article is sitting pretty at the top of the ePrint archive.**



**That one asshole who’s always sleeping during my Eurocrypt talks.**



**The MIT Mafia.**



**The NSA’s massive stack of amateur porn.**



**The North Korean Cryptographic Standard.**



**The awkward question the chair asks when nobody understood the talk.**



**The awkward silence of 8 people standing in a circle during the afternoon coffee break.**



**The great firewall of China.**



**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><b>The great paywall of IEEE.</b></p> <p></p>	<p><b>The intoxicating aroma of 12 PhD students in one office.</b></p> <p></p>	<p><b>The latest dance mix album by DJ Bernstein.</b></p> <p></p>
<p><b>The one person I don't want to get stuck next to on the conference excursion bus.</b></p> <p></p>	<p><b>The one really hot person at CHES registration drinks.</b></p> <p></p>	<p><b>The one suit I own for meetings with industry.</b></p> <p></p>
<p><b>The person in the front row taking photos of every slide.</b></p> <p></p>	<p><b>The secret flash drive hidden in my underwear.</b></p> <p></p>	<p><b>The student body.</b></p> <p></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><b>The walking zombie corpse of Claude Shannon.</b></p> 	<p><b>Thinking I'm so clever for using pictures of Alice (Cooper) and Bob (Marley).</b></p> 	<p><b>Throwing a party for my next citation milestone.</b></p> 
<p><b>Trying to make TCC friends at the bar in order to get the IACR 7-conference grand slam.</b></p> 	<p><b>Turbulent bowel movements in the middle of my Asiacrypt presentation.</b></p> 	<p><b>Turning up to one meeting and claiming co-authorship.</b></p> 
<p><b>Tweeting about my paper acceptance.</b></p> 	<p><b>Unbreakable military-grade encryption.</b></p> 	<p><b>Undergrads.</b></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**

**Using Beamer because it's social suicide to use PowerPoint.**



**Using “it clearly follows” when the implied following is anything but clear.**



**Using “we should talk about this offline” because the question exposes holes in my paper.**



**Using indecipherable, non-standard notation to hide a dodgy proof.**



**Vital sugar beet auctions.**



**WalnutDSA.**



**Wearing a T-shirt with a Linux joke.**



**Wearing a conference t-shirt... in public.**



**When you realize that quantum computers have been 10 years away for 3 decades.**



**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**

**Wistfully looking out of the window of my overly-cramped PhD office.**



**Writing a reference for someone I can't remember meeting.**



**Yet another cryptographer falling into the blockchain startup abyss.**



**Ctrl+F'ing to see how many times I'm cited and finding "0 results".**



**"Working" remotely.**



**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**